User Manual

TAINY HMOD-V2-IO, TAINY HMOD-L1-IO
TAINY EMOD-V2-IO, TAINY EMOD-L1-IO

Dr. Neuhaus

Copyright Statement

The contents of this publication are protected by copyright. Translations, reprints, reproduction and storage in data processing systems require the express permission of Dr. Neuhaus Telekommunikation GmbH.

© 2012 Dr. Neuhaus Telekommunikation GmbH

All rights reserved.

Dr. Neuhaus Telekommunikation GmbH

Papenreye 65, D-22453 Hamburg

Fax.: +49 (40) 55304-180

Internet: http://www.neuhaus.de

E-mail: Kundendienst@neuhaus.de

Subject to technical alterations.

TAINY® is a trademark of Dr. Neuhaus Telekommunikation GmbH. All other trademarks and product designations are trademarks, registered trademarks or product designations of their respective owners.

Dr. Neuhaus Telekommunikation GmbH provides all goods and services on the basis of the General Terms and Conditions of Dr. Neuhaus Telekommunikation GmbH currently valid. All information is based on information provided by the manufacturer(s). No responsibility or liability will be assumed for incorrect or missing entries. The descriptions of the specifications in this manual do not constitute an agreement.

Product no.: 3173, 3183

Doc. no.: 3183AD001 Version 2.1

Products: TAINY HMOD-V2-IO, TAINY EMOD-V2-IO

TAINY HMOD-L1-IO, TAINY EMOD-L1-IO

Firmware-Version 1.309

Safety instructions

Products

The name TAINY xMOD is used hereinafter as a collective term for TAINY HMOD-V2-IO, TAINY HMOD-L1-IO, TAINY EMOD-V2-IO, and TAINY EMOD-L1-IO.

Qualified personnel

The associated device/system may only be set up and operated in conjunction with this documentation. Devices/systems may only be put into service and operated by qualified personnel. For the purposes of the safety instructions in this documentation, qualified personnel are persons who are authorised to put into service, earth and label devices, systems and circuits in accordance with safety engineering standards.

General notes concerning the product

The product TAINY xMOD complies with the European standard EN60950 (11.2006 /A1:2010), Safety of Information Technology Equipment. Read the installation instructions carefully before using the device. Keep the device out of reach of children, especially small children. The device may not be installed or operated outdoors or in damp areas. Do not put the device into operation if connecting cables or the device itself is damaged.

External power supply

Use only an external power supply that also conforms to EN60950. The output voltage of the external power supply must not exceed 60V DC. The output of the external power supply must be short-circuit proof.

The TAINY xMOD may only be supplied via power supplies according to IEC/EN60950 Section 2.5 "Limited Power Source". The external power supply for the TAINY xMOD must comply with the requirements for NEC Class 2 circuits as defined in the National Electrical Code ® (ANSI/NFPA 70).

When connecting to a battery or rechargeable battery, ensure that an all-pole disconnecting device (battery main switch) with sufficient disconnecting capacity and a fuse with sufficient disconnecting capacity (e.g. Paden FKS fuse set 32 V, 3 A, order no. 162.6185.430) is provided between the device and the battery or rechargeable battery.

Observe the section Technical data of this documentation (Chapter 13) and the instructions for installation and use of the respective manufacturers of the power supply, the battery or the rechargeable battery.

In port and switching output

The in port and switching output are both galvanic insulated against all other terminals of the TAINY xMOD. If the external installation being connected to the TAINY xMOD connects a signal of the in port and switching output galvanically to a power supply signal of the TAINY xMOD, the voltage between each signal of the in port and switching output and each signal of the power supply may not exceed 60V.

Handling cables

Never pull on the cable to pull a cable plug out of its socket; instead pull on the plug. Always use edge protectors when routing cables over sharp corners and edges. Provide adequate strain relief for cables when necessary.

For safety reasons, ensure that the bending radii of the cables are observed.

Failure to observe the bending radii of the antenna cable will degrade the device's transmitting and receiving characteristics. The bending radius must not be less than the minimum of 5 times the cable diameter statically and 15 times the cable diameter dynamically.

Wireless device

Never use the device in areas where the operation of wireless equipment is prohibited. The device contains a wireless transmitter that may degrade the function of electronic medical devices such as hearing aids or pacemakers. Please consult your physician or the manufacturer of such devices. To prevent demagnetisation of data storage media, do not place any floppy disks, credit cards or other magnetic data storage media near the device.

Antenna installation

The recommended radiological limits of the German Commission on Radiological Protection (Strahlenschutzkommission) of 13/14 September 2001 must be complied with.

Installing an outdoor antenna

When installing an antenna outdoors, the antenna must be installed properly by qualified personnel. Lightning protection standard DIN EN 62305 part 1 to 4 in their currently valid version and further standards must be complied with.

The EMC lightning protection zone concept according to DIN EN 62305-4

The EMC lightning protection zone concept must be observed. In order to avoid large induction loops, lightning protection equipotential bonding must be used. If the antenna or the antenna cable is installed in the area of the lightning protection system, then the minimum distances from the lightning protection system must be observed. If this is not possible, then isolated installation as described in lightning protection standard DIN EN 62305 part 1 to 4in their currently valid version is absolutely essential.

RF exposure

RF exposure

Normally the antenna connected to this device's transmitter works in all directions with 0 dB amplification. The composite power in PCS mode is less than 1 watt ERP when this antenna is used.

The internal / external antennas used with this mobile devices must be at least 20 cm from persons, and they may not be placed or operated so that they work in a combination with another antenna or transmitter.

Radio interference

The TAINY xMOD is a Class A device. This device can cause radio interference in residential areas; in this case the user may be required to take appropriate measures.

Warning about costs

Please note that data packets which are subject to charges are exchanged even when a connection is (re-) established, when an attempt to connect to a remote station is made (e.g. server is switched off, wrong destination address, etc.), and to maintain a connection.

In example, a remote station which is not available may cause significant unwanted costs, because of a great number of connection retries, being not successful.

Firmware with open source GPL/LGPL

The firmware for TAINY xMOD contains open source software under GPL/LGPL conditions. We provide you with the source code in accordance with Section 3b of GPL and Section 6b of LGPL. You can find the source code on our webpage, www.neuhaus.de.

As an alternative, you can also request the source code from us on CD-ROM. Send your email to Kundendienst@neuhaus.de. Please enter "Open Source xMOD" in the subject line of your email so that we can easily filter out your message.

The license conditions for the open source software can be found in the source code on the product CD.

Firmware with OpenBSD

The firmware of the TAINY xMOD contains parts from the OpenBSD software. Whenever OpenBSD software is used, the following copyright note must be reproduced:

```
* Copyright (c) 1982, 1986, 1990, 1991, 1993
* The Regents of the University of California. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must display the following acknowledgement:
*    This product includes software developed by the University of
*    California, Berkeley and its contributors.
* 4. Neither the name of the University nor the names of its contributors
*    may be used to endorse or promote products derived from this software
*    without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
* CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
* WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
```

A word from our technical service

We, the customer service technicians of Dr. Neuhaus Telekommunikation GmbH, offer you our cordial greetings. If you have any difficulties in putting your new device into operation, we will be your contacts, and will be glad to help you. Even if you have a special or unusual combination of hardware and software, and there is something that you cannot get to work right away, you can always turn to us. Our products' good reputation depends on our customers always being able to get help from a team of experienced specialists, who can also deal with unusual combinations. You can reach us at **Kundendienst@neuhaus.de**.

Environmental protection is also important to us

Maintaining an environment worth living in, i.e. to join ecology and economics in an appropriate way, is one of the most important tasks of our times. We meet this challenge in the following ways:

Quality

Requirements-oriented development and production, firmly rooted in state-of-the-art quality assurance mechanisms, ensure products of the highest quality which can remain in use for a long time.

Return guarantee

We are proud of our products. All the same, we acknowledge that they do not last forever. That is why wherever it is technically possible and feasible we manufacture all of our products of recyclable materials. We guarantee that we will take back any device manufactured by us, send the re-usable parts for recycling, and dispose of the rest in an environmentally friendly manner. Please contact our Service Center

Dr. Neuhaus Telekommunikation GmbH
Service-Zentrum
Messestraße 20,
D-18069 Rostock

Please help us to protect the environment.

Dr. Neuhaus Telekommunikation GmbH

Contents

1 Introduction 9
2 Setup 14
2.1 Step by step 14
2.2 Preconditions for operation 15
2.3 Overview 16
2.4 Service button 16
2.5 Operating state indicators 17
2.6 Connections 20
2.7 Inserting the SIM card 22
3 Configuration 23
3.1 Overview 23
3.2 Allowed characters for user name, passwords and other inputs 23
3.3 TCP/IP configuration of the network adapter in Windows XP 24
3.4 Establishing a configuration connection 25
3.5 Status overview (start page) 28
3.6 Configuration procedure 30
3.7 Configuration Profiles 31
3.8 Changing the password 32
3.9 Reboot 33
3.10 Load factory settings 34
3.11 Device identification 34
4 Local interface 35
4.1 IP addresses of the local interface 35
4.2 DHCP server to local network 35
4.3 DNS to local network 37
4.4 Local hostname 38
4.5 System Time/NTP 38
4.6 Additional Internal Routes 39
5 External interface 40
5.1 Network selection and access parameters for UMTS/GPRS 40
5.2 UMTS/GPRS connection monitoring 44
5.3 Hostname via DynDNS 45
5.4 Secure DynDNS 46
5.5 NAT – Network Address Translation 47
5.6 Installation mode 48
5.7 Volume supervision 49
6 Security functions 50
6.1 Packet Filter 50
6.2 Port Forwarding 53

6.3 Advanced security functions 54
6.4 Firewall Log 55
7 VPN connections 56
7.1 Introduction 56
7.2 VPN Roadwarrior Mode 58
7.3 VPN IPsec Standard Mode 62
7.4 Loading VPN certificates 69
7.5 Firewall rules for VPN tunnel 70
7.6 Supervision of VPN connections 71
7.7 Advanced settings for VPN connections 73
7.8 Status of the VPN connections 74
8 Remote access 75
8.1 HTTPS remote access 75
8.2 Remote access – SSH 76
8.3 Remote access via dial-in connection 78
9 Status, log and diagnosis 80
9.1 Log 80
9.2 Remote logging 81
9.3 Snapshot 82
9.4 Hardware information 83
9.5 Software information 83
9.6 Software Update 84
10 Additional functions 85
10.1 SMS Service Center 85
10.2 Alarm SMS 85
10.3 SMS – Messaging from the local network 86
11 SNMP 89
11.1 Operation via SNMP 89
11.2 Alarm messages via SNMP traps 91
12 Small lexicon of routers 93
13 Technical data 107
13.1 TAINY HMOD-V2-IO, TAINY HMOD-L1-IO 107
13.2 TAINY EMOD-V2-IO, TAINY EMOD-L1-IO 109

1 Introduction

Products

This manual provides security instructions and describes the operation and installation of the following products:

	VPN Function	HSDPA / UMTS	E-GPRS	GPRS	CSD
TAINY HMOD-V2-IO	**X**	**X**	**X**	**X**	**X*)**
TAINY HMOD-L1-IO	**-**	**X**	**X**	**X**	**X*)**
TAINY EMOD-V2-IO	**X**	**-**	**X**	**X**	**X**
TAINY EMOD-L1-IO	**-**	**-**	**X**	**X**	**X**

*) Only if not registered to a HSDPA / UMTS network

Product names used

The following collective terms are used in this manual for the various TAINY product versions:

TAINY xMOD	Collective term for TAINY HMOD-V2-IO, TAINY HMOD-L1-IO, TAINY EMOD-V2-IO, TAINY EMOD-L1-IO.
TAINY HMOD	Collective term for TAINY HMOD-V2-IO and TAINY HMOD-L1-IO.
TAINY EMOD	Collective term for TAINY EMOD-V2-IO and TAINY EMOD-L1-IO.
TAINY xMOD-V2-IO	Collective term for TAINY HMOD-V2-IO and TAINY EMOD-V2-IO.
TAINY xMOD-L1-IO	Collective term for TAINY HMOD-L1-IO and TAINY EMOD-L1-IO.

Application

The TAINY xMOD provides a wireless connection to the internet or to a private network.

The TAINY HMOD provides this connection anywhere a UMTS network (Universal Mobile Telecommunication System = 3rd generation mobile communications network) or a GSM network (Global System for Mobile Communication = mobile communications network) which provides IP-based data service is available. For UMTS, this means the HSDPA data service (High Speed Download Data Access) or the UMTS Data Service- For GSM, this means EGPRS (Enhanced General Packet Radio Service = EDGE) or GPRS (General Packet Radio Service).

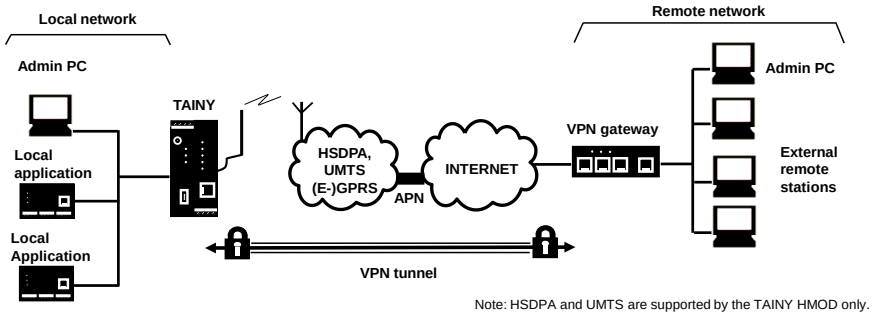
The TAINY EMOD provides this connection anywhere a GSM network (Global System for Mobile Communication = mobile communications network) is available, which provides EGPRS (Enhanced General Packet Radio Service = EDGE) or GPRS (General Packet Radio Service) as a service. This requires a SIM card from a mobile network operator with services activated accordingly.

The TAINY xMOD-L1-IO connects a locally connected application or entire networks to the internet using wireless IP connections. Direct connection can also be made to an intranet which the external remote stations are connected to.

The TAINY xMOD-V2-IO can establish a VPN (Virtual Private Network) between a locally connected application/network and an external network using a wireless IP connection and can protect this connection from third party access using IPsec (Internet Protocol Security).

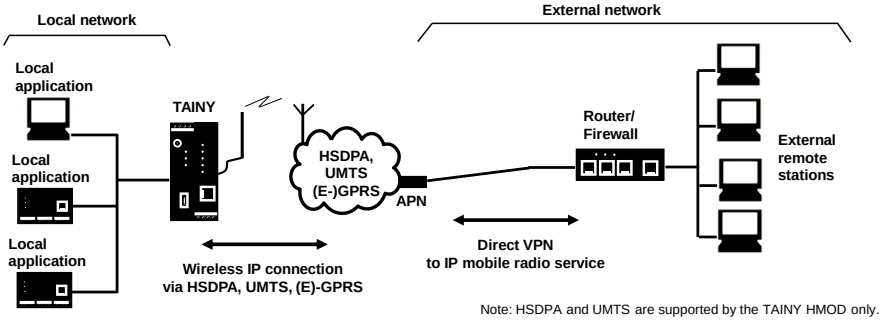
Scenario 1: Virtual Private Network (VPN) with IPsec

TAINY xMOD-V2-IO only



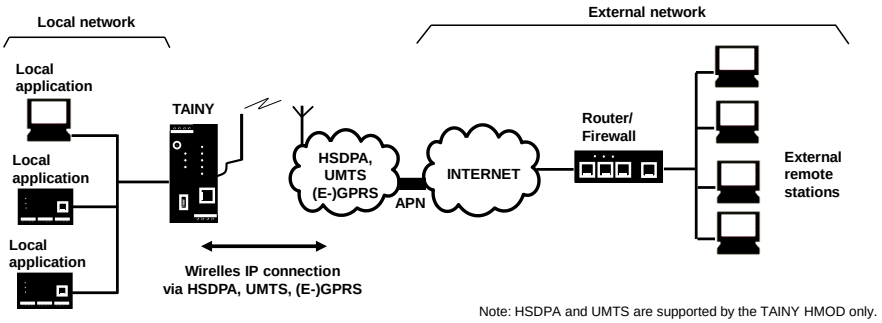
Note: HSDPA and UMTS are supported by the TAINY HMOD only.

Scenario 2: Connection via HSDPA, UMTS, EGPRS or GPRS and a direct VPN to an external network:



Note: HSDPA and UMTS are supported by the TAINY HMOD only.

Scenario 3: Connection via HSDPA, UMTS, EGPRS or GPRS and the Internet to an external network:



Note: HSDPA and UMTS are supported by the TAINY HMOD only.

Local applications could be, for example, a programmable controller, a machine with an Ethernet interface for remote monitoring, or a notebook or desktop PC. These applications use the TAINY xMOD in order to access an external network just as if they had a direct, local connection to this external network.

Functions

In order to perform these tasks in the scenarios described, the device combines the following functions:

	TAINY HMOD		TAINY EMOD	
	V2-IO	L1-IO	V2-IO	L1-IO
HSDPA / UMTS	X	X	-	-
EGPRS / GPRS / CSD	X*)	X*)	X	X
VPN functions	X	-	X	-
Firewall	X	X	X	X
Configuration	X	X	X	X
Further functions	X	X	X	X

*) Only if not registered to a HSDPA / UMTS network

Communication

Wireless modem for flexible data communication in UMTS networks

- via HSDPA, UMTS

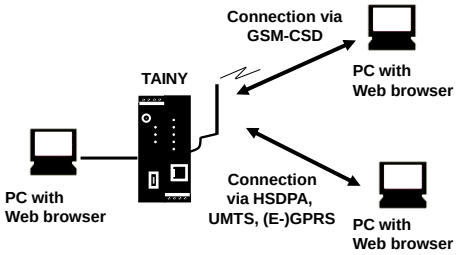
Wireless modem for flexible data communication in GSM networks

- EGPRS, GPRS (and CSD)

Configuration

The device can be configured via a Web user interface that can simply be displayed using a Web browser. It can be accessed by means of the following:

- the local interface,
- HSDPA, UMTS, EGPRS, GPRS, or
- CSD (Circuit Switched Data = dial-in data connection) of the GSM



Note: HSDPA and UMTS are supported by the TAINY HMOD only.

VPN functions

The TAINY HMOE-V2-IO and the TAINY EMOD-V2-IO provide the following VPN features

- VPN router for secure data transfer via public networks
- Protocol: IPsec (tunnel mode)
- IPsec-3DES encryption with 192 Bit
- IPsec-AES encryption with 128, 192 and 256 bit
- Package authentication: MD5, SHA-1
- Internet Key Exchange (IKE) with main and aggressive mode
- Authentication: Pre-Shared Key (PSK), X.509v3 certificate, CA
- NAT-T
- 1-to-1 NAT
- Dead Peer Detection (DPD)
- Switching output for indicating an established VPN tunnel

Firewall functions

The TAINY xMOD provides the following firewall functions in order to protect the local network and itself from external attacks:

- Stateful inspection firewall
- Anti-spoofing
- Port forwarding

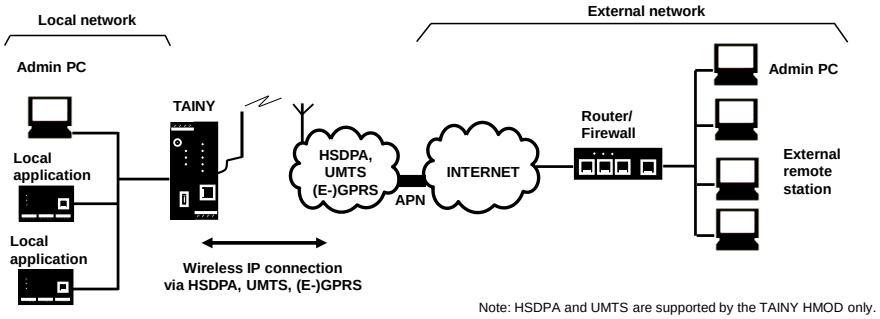
Additional functions

The TAINY xMOD provides the following additional functions:

- DNS cache
- DHCP server
- NTP
- Remote logging
- In Port
- Web user interface for configuration
- Sending alarm SMSes
- Sending SNMP traps
- Send SMSes from local network
- SSH console for configuration
- SNMP for control and configuration
- DynDNS client
- Dial-in data connection for maintenance and remote configuration
- Volume monitoring
- Installation mode for antenna alignment

Terms

Here are definitions of terms frequently used in this manual:



Note: HSDPA and UMTS are supported by the TAINY HMOD only.

Local network

Network connected to the local interface of the TAINY xMOD. The local network contains at least one local application.

Local interface

Interface of the TAINY xMOD for connecting the local network. The interface is labelled 10/100 Base-T on the device. This is an Ethernet interface with a data rate of 10Mbit/s or 100Mbit/s (Autosensing MDI/MDIX).

Local application
Local applications are network components in the local network, for example a programmable controller, a machine with an Ethernet interface for remote monitoring, or a notebook or desktop PC or the Admin PC.

Admin PC
Computer with Web browser (e.g. MS Internet Explorer Version 7 or later or Mozilla Firefox Version 2 or later) connected to the local network or the external network; used to configure the TAINY xMOD. The Web browser must support HTTPS. Device configuration via SSH requires an SSH client on the Admin PC, for example putty.

External network
External network which the TAINY HMOD is connected to via HSDPA, UMTS, EGPRS or GPRS. External networks are the internet or a private intranet.

External network which the TAINY EMOD is connected to via EGPRS or GPRS. External networks are the internet or a private intranet.

External remote stations
External remote stations are network components in an external network, e.g. Web servers on the Internet, routers on an intranet, a central company server, an Admin PC, and much more.

(E-)GPRS
EGPRS or GPRS depending on what services are available.

VPN gateway
Component of the external remote network that supports IPsec and which is compatible with the TAINY HMOD-V2-IO and the TAINY EMOD-V2-IO

Remote network
External network with which the TAINY xMOD is establishing a VPN connection.

Mobile communications network
Infrastructure and technology for wireless mobile verbal and data communication.

The TAINY HMOD is designed for use in UMTS mobile communications networks and GSM mobile communications networks,

The TAINY EMOD is designed for use in EDGE/GSM mobile communications networks.

Mobile data service
Data transmission services provided by the mobile communications network which can be used by the TAINY xMOD:

	TAINY HMOD		TAINY EMOD	
	V2-IO	L1-IO	V2-IO	L1-IO
UMTS wireless net	X	X	-	-
HSDPA	X	X	-	-
UMTS data	X	X	-	-
GSM wireless net (with EDGE)	X	X	X	X
E-GPRS	X	X	X	X
GPRS	X	X	X	X
CSD	X*)	X*)	X	X

*) Only if not registered to a HSDPA / UMTS network

2 Setup

2.1 Step by step

Set up the TAINY xMOD in the following steps:

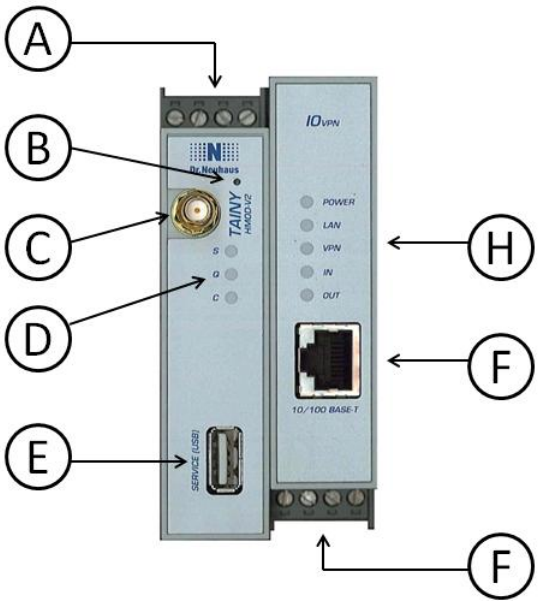
Step		Chapter
1.	First familiarise yourself with the preconditions for operation of the TAINY xMOD.	2.2
2.	Read the safety instructions and other instructions at the beginning of this user manual very carefully, and be sure to follow them.	
3.	Please familiarise yourself with the control elements, connections and operating state indicators of the TAINY xMOD.	2.3 to 2.6
4.	Connect a PC with a Web browser (Admin PC) to the local interface (10/100 BASE-T) of the TAINY xMOD.	3.3, 3.4
5.	Using the Web user interface of the TAINY xMOD, enter the PIN (Personal Identification Number of the SIM card.	5.1
6.	Disconnect the TAINY xMOD from the power supply.	2.6
7.	Insert the SIM card in the device.	2.7
8.	Connect the antenna.	2.6
9.	Connect the TAINY xMOD to the power supply.	2.6
10.	Set the TAINY xMOD up in accordance with your requirements.	3 to 101
11.	Connect your local application.	2.6

2.2 Preconditions for operation

In order to operate the TAINY xMOD, the following information must be on hand and the following preconditions must be fulfilled:

Antenna	An antenna, adapted to the frequency bands of the GSM network operator you have chosen: 850 MHz, 900 MHz, 1800 MHz or 1900 MHz. Please use only antennas from the accessories for the TAINY xMOD, because they are tested to operate together with the TAINY xMOD. See Chapter 2.6.
Power supply	A power supply with a voltage between 12 V_{DC} and 60 V_{DC} that can provide sufficient current. See Chapter 2.6.
SIM card	A SIM card from the chosen GSM network operator.
PIN	The PIN for the SIM card
HSDPA / UMTS EGPRS / GPRS activation	The services HSDPA, UMTS data (only TAINY HMOD) and / or EGPRS or GPRS must be enabled on the SIM card by your mobile communications network provider. The access data must be known: - Access Point Name (APN) - User name - Password
CSD 9600 bit/s activation	The SIM card must be activated by your GSM network operator for the CSD service if you wish to use remote configuration via a dial-in data connection, see Chapter 8.3.

2.3 Overview



A – Connection terminals for the power supply

B – Service button

C – Antenna jack type SMA

D – Operating state indicators S, Q, C

E – Service (USB) – reserved for later applications

F – Connection terminals for the gate inputs and outputs

G – 10/100 Base-T - RJ45 jack for connecting the local network

H – Operating state indicators POWER, VPN, LAN, IN, OUT

2.4 Service button

On the front side of the TAINY xMOD there is a small hole (see B) which has a button behind it. Use a pointed object, e.g. a straightened-out paperclip, to press this button.

- If you press the button for longer than 5 seconds, the TAINY xMOD reboots and loads the factory settings.

2.5 Operating state indicators

The TAINY xMOD-V2-IO has eight indicator lamps (LEDs), while the TAINY xMOD-L1-IO has seven indicator lamps (LEDs) for displaying the operating status.

The three indicator lamps on the left half of the device indicate the status of the wireless modem:

TAINY HMOD

Lamp	State	Meaning
S *(Status)*	Flashing slowly	PIN transfer
	Flashing quickly	PIN error / SIM error
	ON	PIN transfer successful
Q *(Quality)*	OFF	Not logged into GSM network
	Flashing briefly	Poor signal strength (CSQ < 6)
	Flashing slowly	Medium signal strength (CSQ= 6..10)
	ON, with brief interruptions	Good signal strength (CSQ=11-18)
	ON	Very good signal strength (CSQ > 18)
C *(Connect)*	OFF	No connection
	Flashing quickly	Service call via CSD active
	Flashing slowly	EGPRS / GPRS connection active
	ON	HSDPA / UMTS connection active
S, Q, C together	Light up in sequence quickly	Booting
	Light up in sequence slowly	Update
	Flashing quickly in unison	Error

TAINY EMOD

Lamp	Status	Meaning
***S** (Status)*	Flashing slowly	PIN transfer
	Flashing quickly	PIN error / SIM error
	ON	PIN transfer successful
***Q** (Quality)*	OFF	Not logged into GSM network
	Flashing briefly	Poor signal strength (CWQ < 6)
	Flashing slowly	Medium signal strength (CSQ 6..10)
	ON with brief interruptions	Good signal strength (CSQ=11-18)
	ON	Very good signal strength (CSQ > 18)
***C** (Connect)*	OFF	No connection
	Flashing quickly	Service call via CSD active
	ON with brief interruptions	GPRS connection active
	ON	EGPRS connection active
S, Q, C together	Light up in sequence quickly	Booting
	Light up in sequence slowly	Update
	Flashing quickly in unison	Error

TAINY xMOD-V2-IO

The 5 indicator lamps on the right-hand side of the device indicate the state of additional device functions:

Lamp	State	Meaning
POWER	ON	Device switched on, operating voltage present
	OFF	Device switched off, operating voltage not present
LAN	ON	Ethernet connection established to the local application / the local network
	OFF	No Ethernet connection to the local application / the local network
	ON with brief interruptions	Data transfer via the Ethernet connection
VPN	ON	At least one VPN connection established
	OFF	No VPN connection established
IN	ON	In port active
	OFF	In port not active
OUT	ON	If the switching output is active.
	OFF	If the switching output is not active.

TAINY xMOD-L1-IO

The four indicator lamps on the right half of the device indicate the following additional device functions:

Lamp	Status	Meaning
POWER	ON	Device switched on, operating voltage present
	OFF	Device switched off, operating voltage not present
LAN	ON	Ethernet connection established to the local application / the local network
	OFF	No Ethernet connection to the local application / the local network
	ON with brief interruptions	Data transfer via the Ethernet connection
IN	ON	Switching input active
	OFF	Switching input not active
OUT	ON	Reserved for future applications
	OFF	Reserved for future applications

2.6 Connections

10/100 Base-T

The local network is connected to the local applications at the 10/100 Base-T connection, e.g. a programmable controller, a machine with an Ethernet interface for remote monitoring, or a notebook or desktop PC.

To set up the TAINY xMOD, connect the Admin PC with Web browser here.

The interface supports autonegation. It is thus detected automatically whether a transmission speed of 10 Mbit/s or 100 Mbit/s is used on the Ethernet.

A connecting cable with a RJ45 plug must be used. It can be wired cross-over or one-to-one.

Service (USB)

In the TAINY xMOD this interface has no function and is reserved for later applications. Please do not connect any devices here. Doing so could interfere with the TAINY xMOD operation.

SMA antenna jack

The TAINY xMOD has an antenna jack of the type SMA for connecting the antenna.

The antenna that is used should have an impedance of about 50 ohms. It must be matched for GSM 900MHz, DCS 1800MHz, UMTS 2100MHz or GSM 850 MHz and PCS 1900 MHz, depending on which frequency bands your mobile radio network operator uses. In Europe and China GSM 900MHz and DCS 1800MHz are used for GSM and 2100 MHz is used for UMTS, in the USA GSM 850 MHz and PCS 1900 MHz are used for GSM and UMTS. Please obtain this information from your network operator.

The match (VSWR) of the antenna must be 1:2.5 or better.

Caution:

Please use only antennas from the accessories line for TAINY xMOD. Other antennas could interfere with product characteristics or even lead to defects.

When installing the antenna, a sufficiently good signal quality must be ensured (CSQ > 11). Use the indicator lamps of the TAINY xMOD which show the signal quality or installation mode, see chapter 5.6 Please make sure that there are no large metal objects (e.g. reinforced concrete) close to the antenna.

Please observe the installation and user instructions for the antenna being used

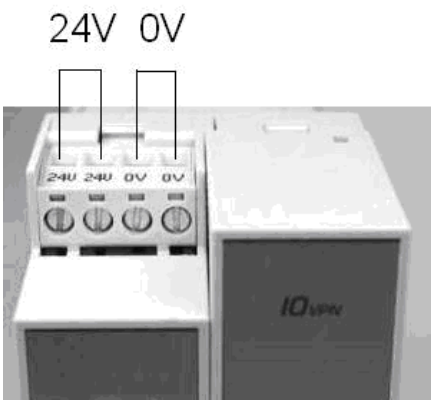
Warning:

When the antenna is installed outdoors it must be earthed for lightning protection. This work must be carried out by qualified personnel.

.

Screw terminals

Power supply



In port and switching output

24V / 0V power supply

The TAINY xMOD operates with direct current of from 12-60 V DC, nominally 24 V DC. This power supply is connected at the screw terminals on the left-hand side of the device.

The current consumption is about 450mA at 12V and 100mA at 60V.

Warning:

The power supply unit of the TAINY HMOD-V2-IO is not isolated.

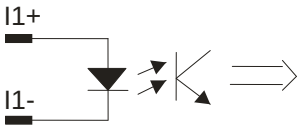
Please observe the safety instructions at the beginning of this manual.

Note:

Make sure that the supply source is sufficiently dimensioned. Instable operation may occur if the supply is too weak.

In port
I1+/ I1-

The TAINY xMOD has an In port. The In port has connections at the screw terminals on the right-hand side of the device. The terminals are designated I1+/I1-.



U_{In} = 5 …30V; ON: $U_{In} \geq$ 5 V; OFF: $U_{In} \leq$ 1,2 V

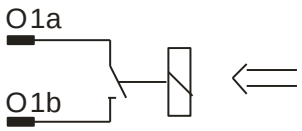
For more on the function of the In port, see also Chapter 10.

Warning:

The In port is galvanically insulated against all other terminals of the TAINY xMOD. If the external installation being connected to the TAINY xMOD connects a signal of the In port galvanically to a power supply signal of the TAINY xMOD, the voltage between each signal of the In port and each signal of the power supply may not exceed 60V.

Switching output O1a/ O1b

The TAINY xMOD-V2-IO has a switching output. The switching output has its connections at the screw terminals on the right-hand side of the device. The terminals are designated O1a/O1b.



U_{Max} = 30V; I_{Max} = 20mA

The switching output is active (switch closed) if at least one VPN connection is established.

The switching output is not active (switch opened) if no VPN connection is established.

Warning:

The switching output is galvanically insulated against all other terminals of the TAINY xMOD. If the external installation being connected to the TAINY xMOD connects a signal of the switching output galvanically to a power supply signal of the TAINY xMOD, the voltage between each signal of the switching output and each signal of the power supply may not exceed 60V.

2.7 Inserting the SIM card

Caution:

Before inserting the SIM card, enter the PIN of the SIM card in the TAINY xMOD via the Web user interface. See Chapter 5.1

1. After you have entered the PIN of the SIM card, disconnect the TAINY xMOD completely from the power supply.
2. The drawer for the SIM card is located on the back of the device. Right next to the drawer for the SIM card in the housing aperture there is a small yellow button. Press on this button with a pointed object, for example a pencil.

   When the button is pressed the SIM card drawer comes out of the housing.
3. Place the SIM card in the drawer so that its gold-plated contacts remain visible.
4. Then push the drawer with the SIM card completely into the housing.

Caution!

Do not under any circumstances insert or remove the SIM card during operation. Doing so could damage the SIM card and the TAINY xMOD.

3 Configuration

3.1 Overview

Configuration of the router and firewall functions is carried out locally or remotely via the Web-based administration interface of the TAINY xMOD. The VPN function can also be configured for the TAINY xMOD-V2-IO.

Remote configuration

Remote configuration via HTTPS or CSD access is only possible if the TAINY xMOD is configured for remote access. In this case proceed exactly as described in Chapter 7.

Configuration via the local interface

The preconditions for configuration via the local interface are:

- The computer (Admin PC) that you use to carry out configuration must be either:
  - connected directly to the Ethernet jack of TAINY xMOD via a network cable

  or
  - it must have direct access to the TAINY xMOD via the local network.
- The network adapter of the computer (Admin PC) that you use to carry out configuration must have the following TCP/IP configuration:

  IP address: **192.168.1.2**

  Subnet mask: **255.255.255.0**

  Instead of the IP address **192.168.1.2** you can also use other IP addresses from the **range 192.168.1.x**. but not 192.168.1.1, 192.168.1.0 und 192.168.1.255.
- If you also wish to use the Admin PC to access the external network via the TAINY xMOD, the following additional settings are necessary:

  Standard gateway: **192.168.1.1**

  Preferred DNS server: **Address of the domain name server**

3.2 Allowed characters for user name, passwords and other inputs

For user names, passwords, host names, APN and PIN the following ASCII characters may be used:

User names, passwords and PIN

! $ % & ' ( ) * + , . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ _ ` a b c d e f g h I j k l m n o p q r s t u v w x y z { | }

Host names and APN

0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h I j k l m n o p q r s t u v w x y z . -

3.3 TCP/IP configuration of the network adapter in Windows XP

Windows Connect To…

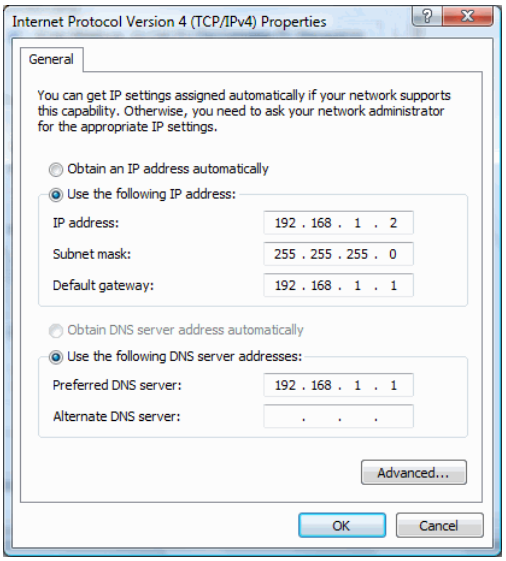
Click on *Start, Connect To ..., Show All Connections…*

Then click on *LAN Connection.* In the dialog box *Properties of LAN Connection*, click on the *General* tab and select there the entry *Internet Protocol (TCP/IP).* Open *Properties* by clicking on the corresponding button.

The window *Properties of Internet Protocol (TCP/IP)* appears (see illustration below).

Note:

The path leading to the dialog box *Properties of LAN Connection* depends on your Windows settings. If you are not able to find this dialog box, please search in the Windows Help function for *LAN Connection* or *Properties of Internet Protocol (TCP/IP)*.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 1 . 2
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
192 . 168 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
192 . 168 . 1 . 1
Alternate DNS server:
Advanced...
OK
Cancel

Enter the following values in order to get to the Web user interface of the TAINY xMOD:

IP address: **192.168.1.2**

Subnet mask: **255.255.255.0**

In addition, enter the following values if you want to use the Admin PC to access the external network via the TAINY xMOD:

Standard gateway: **192.168.1.1**

Preferred DNS server: **Address of the Domain Name Servers**

Preferred DNS server

If you call up addresses via a domain name (e.g. www.neuhaus.de), then you must refer to a domain name server (DNS) to find out what IP address is behind the name. You can define the following as the domain name server:

- The DNS address of the network operator,

  or

- The local IP address of the TAINY xMOD, as long as it is configured for breaking out host names into IP addresses (see Chapter 4.3). This is the **factory setting**.

To define the domain name server in the TCP/IP configuration of your network adapter, proceed as described above.

3.4 Establishing a configuration connection

Setting up a Web browser

Proceed as follows:

1. Launch a Web browser.

   (e.g. MS Internet Explorer Version 7 or later or Mozilla Firefox Version 2 or later; the Web browser must support SSL (i.e. HTTPS).)

2. Make sure that the browser does not automatically dial a connection when it is launched.

   In MS Internet Explorer 7, make this setting as follows: Menu *Tools, Internet Options...*, tab *Connections*: The option *Do not select a connection* must be activated.

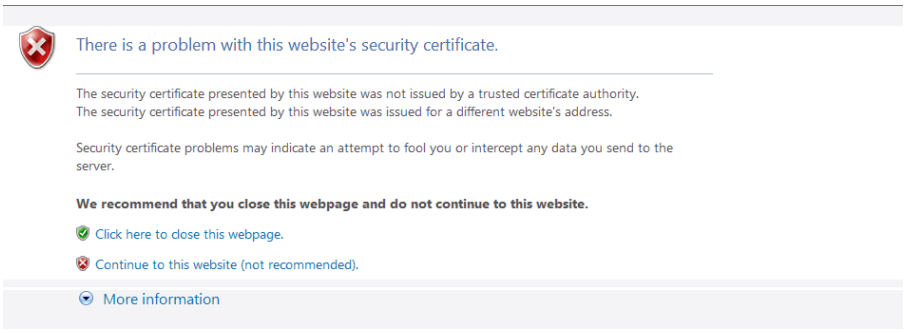
Calling up the start page of the TAINY xMOD

3. In the address line of the browser, enter the address of the TAINY xMOD in full. In the factory settings this is:

   https://192.168.1.1

   Result: A security message appears. In Internet Explorer 7, for example, this one:

Confirming the security message


There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

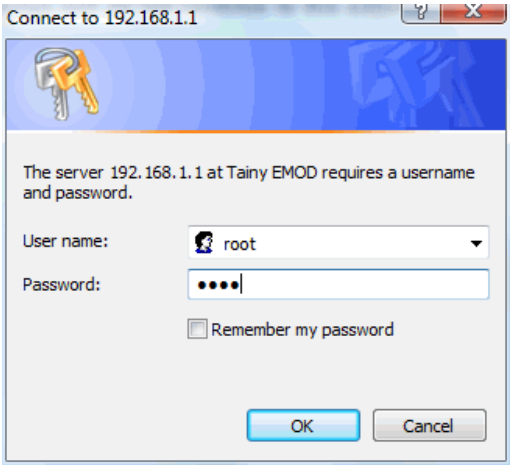
4. Acknowledge the corresponding safety message with "Continue loading this page …"

Note

Because the device can only be administered via encrypted access, it is delivered with a self-signed certificate. In the case of certificates with signatures that the operating system does not know, a security message is generated. You can display the certificate.
It must be clear from the certificate that it was issued for Dr. Neuhaus Telekommunikation GmbH. The Web user interface is addressed via an IP address and not using a name, which is why the name specified in the security certificate is not the same as the one in the certificate.

5. You will be asked to enter the user name and the password:

Entering the user name and password



The factory setting is:

User name: **root**

Password: **root**

Note

You should change the password in any event. The factory setting is general knowledge and does not provide sufficient protection. Capital 3.8 contains a description of how to change the password.

The start page is displayed

After the user name and password are entered, the start page of the TAINY xMOD appears in the Web browser with an overview of the operating state, see Chapter 3.5.

The start page is **not** displayed

If after several tries the browser still reports that the page cannot be displayed, try the following:

- Check the hardware connection. On a Windows computer, go to the DOS prompt (Menu *Start, Programs, Accessories, Command Prompt*) and enter the following command:

  ping 192.168.1.1

  If a return receipt message for the 4 packets that were sent out does not appear within the specified time period, please check the cable, the connections and the network card.

- Make sure that the browser does not use a proxy server. In MS Internet Explorer (Version 7.0), make this setting as follows: Menu *Tools, Internet Options...*, tab *Connections*: Under *LAN Settings*, click on the *Settings...* button, then in the dialog box *Settings for local network (LAN)*, make sure that under *Proxy Server* the entry *Use proxy server for LAN* is not activated.

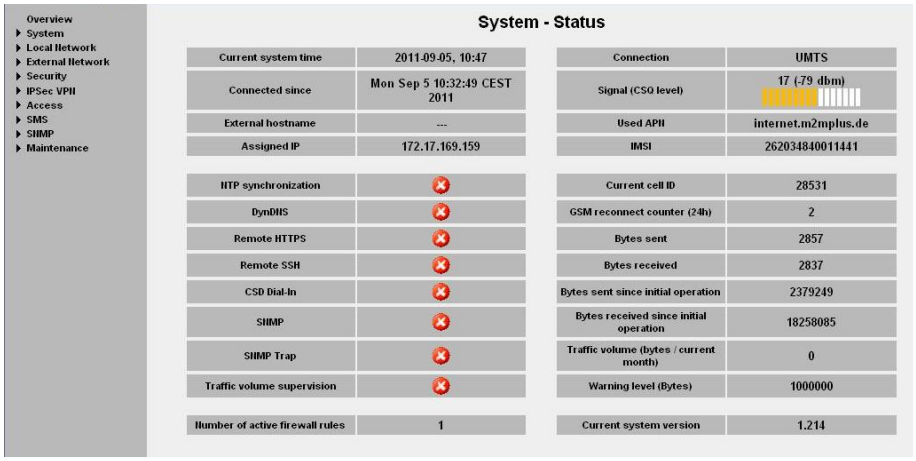
- If other LAN connections are active on the computer, deactivate them for the duration of the configuration process.
  Under the Windows menu *Start, Connect To ..., Show All Connections…* , under LAN or High-Speed Internet right-click on the connection concerned and select *Deactivate* in the pop-up menu.

- Enter the address of the TAINY xMOD with a slash:

  https://192.168.1.1/

3.5 Status overview (start page)

Overview



After the Web user interface of the TAINY xMOD is called up and the user name and password are entered, an overview of the current operating state of the TAINY xMOD appears.

Note

Use the *Refresh* function of the Web browser to update the displayed values.

Current system time — Displays the TAINY xMOD's current system time in the format:

Year – Month – Day, Hours – Minutes

Connection — Shows how long the current connection to the mobile data service has been established.

External hostname — Displays the TAINY xMOD's host names (e.g. tainy.mydns.org), if a DynDNS service is used.

Assigned IP address — Shows the IP address which the TAINY xMOD can be reached at through the mobile data service. This IP address is assigned to the TAINY xMOD by the mobile data service.

Connection — Indicates if and which wireless connection is established.

For TAINY HMOD:

- UMTS connection (IP connection via HSDPA, UMTS data)
- GPRS/EDGE connection (IP connection via EGPRS or GPRS)
- CSD connection (service connection via CSD)

For TAINY EMOD:

- EDGE connection (IP connection via EGPRS)
- GPRS connection (IP connection via GPRS)
- CSD connection (service connection via CSD)

Note

It is possible that a wireless connection and an assigned IP address are displayed, but the connection quality is not good enough to transmit data. For this reason, we recommend using the active connection monitoring (see chapter 0).

Signal (CSQ Level)	Indicates the strength of the GSM signal as a CSQ value and (in parentheses) as an RSSI value in dBm. □ CSQ < 6: Poor signal strength □ CSQ= 6..10: Medium signal strength □ CSQ=11-18: Good signal strength □ CSQ > 18: Very good signal strength □ CSQ = 99: No connection to the mobile network
Used APN	Shows the APN (= Access Point Name) used for the mobile data service.
IMSI	Shows the participant recognition, which is stored on the SIM card in use. The GSM network operator recognises the SIM card's authorisations and agreed services based on the IMSI (= International Mobile Subscriber Identity).
NTP synchronization	Shows whether the NTP synchronization is activated NTP synchronization activated. NTP synchronization not activated.
DynDNS	Shows whether a DynDNS service is activated DynDNS service activated. DynDNS service not activated
Remote HTTPS	Shows whether remote access to the Web user interface of the TAINY xMOD via mobile radio network is permitted (see Chapter 8.1). Access using HTTPS is allowed. Access using HTTPS is not allowed.
Remote SSH	Shows whether remote access to the SSH console of the TAINY HMOD-V2-IO via mobile radio network is permitted (see Chapter 8.2). Access using SSH is allowed. Access using SSH is not allowed.
CSD Dial-In ONLY TAINY EMOD	Shows whether remote CSD service calls are allowed (see Chapter 8.3). □ White hook on red point: CSD service calls are possible. □ White cross on red point: CSD service calls are not possible.
SNMP	Shows whether the setting and reading of parameters via SNMP is enabled (see chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**): Setting/reading of parameters via SNMP is allowed. Setting/reading of parameters via SNMP is not allowed.
SNMP Trap	Shows whether the sending of SNMP messages (SNMP traps) is enabled (see chapter 11.2): Sending of SNMP messages activated.

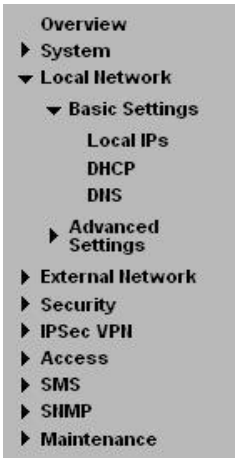
	SNMP messages not activated.
Traffic volume supervision	Shows whether the traffic volume supervision is switched on (see chapter 5.7): Traffic volume supervision is activated. Traffic volume supervision is not activated.
Current Cell ID	Shows the identification of mobile network base station which the TAINY xMOD is currently connected to.
GSM reconnect counter (24h)	Shows the TAINY xMOD'S number of login attempts to the APN since 0:00 (system time). The value 0 indicates that no repeat login attempts have taken place.
Bytes sent / Bytes received	Shows the number of bytes which have been sent or received during the present connection via the mobile data service. The counter is reset when a new connection is established.
	Note These figures merely serve as an indication of the data volume and may deviate from the calculation of the network operator.
Bytes sent / Bytes received since initial operation	Shows the number of bytes which have been sent or received via the mobile data service since the factory settings were most recently loaded. The counters are reset when the factory settings are loaded.
Traffic volume (bytes / current month)	Shows the number of bytes sent and received since the beginning of the month (system time).
	Note These figures merely serve as an indication of the data volume and may deviate significantly from the calculation of the GSM network operator. The NTP synchronization must be activated.
Warning level (Bytes)	Shows the warning level set for the data volume, at which point the TAINY xMOD sends a message.
Number of active firewall rules	Shows how many firewall rules are activated.
Current system version	Shows the version number of the TAINY xMOD's software.

3.6 Configuration procedure

The procedure for configuration is as follows:

Carrying out configuration

1. Use the menu to call up the desired settings area
2. Make the desired entries on the page concerned or use **Reset** to delete the current entry which has not been saved.
3. Use **Save** to confirm the entries so that they are accepted by the device.



ONLY TAINY HMOD-V2-IO

ONLY TAINY EMOD-V2-IO

Note regarding the scope of function

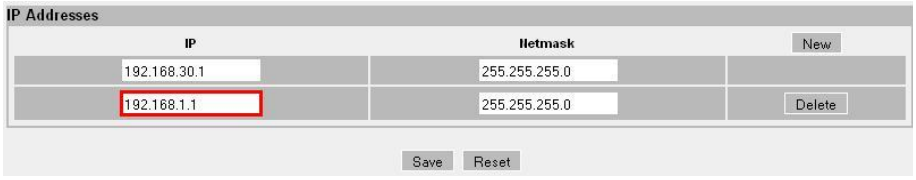
The menu item IPsec-VPN is only present for the TAINY HMOD-V2-IO and TAINY EMOD-V2-IO.

➲ Depending on how you configure the TAINY xMOD, you may then have to adapt the network interface of the locally connected computer or network accordingly.

➲ When entering IP addresses, always enter the IP address component numbers without leading zeros, e.g.: 192.168.0.8.

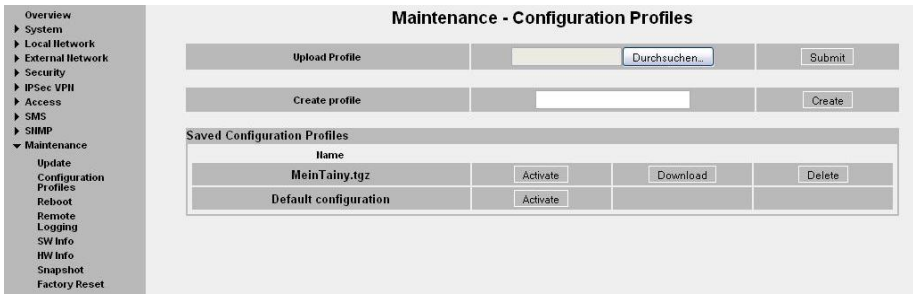
Invalid entries

The TAINY xMOD checks your entries. Obvious errors are detected during saving and the input box in question is marked. The entered value is reset to the default value.



3.7 Configuration Profiles

Maintenance > Configurations Profiles



Function

The settings of the TAINY xMOD can be saved in configuration profiles (files) and re-loaded at any time.

Upload Profile

Loads to the TAINY xMOD a configuration profile that was created before and saved on the Admin PC. Files with configuration profiles have the file extension *.tgz.

Browse can be used to search the Admin PC for configuration profiles,

Submit loads the configuration profile to the TAINY xMOD.

It will then be shown in the table of saved configuration profiles.

Create profile

Saves the current settings of the TAINY xMOD in a configuration profile.

First enter a name for the profile in the input box. *Create* saves the settings in a profile with this names and then displays them in the table of saved configuration profiles.

The following characters may be used for the name:

( ) . - 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ ] _ a b c d e f g h I j k l m n o p q r s t u v w x y z

Create saves the settings in a profile with this name and then shows them in the table of saved configuration profiles.

Saved Configuration Profiles

The table of saved configuration profiles shows all of the profiles that are saved in the TAINY xMOD.

Download Loads the profile to the Admin PC.

Activate The TAINY xMOD accepts the settings from the selected configuration profile and continues to work using them.

Delete The configuration profile is deleted.

The profile *Default configuration* contains the factory settings, and cannot be deleted.

Loading and activating configuration profiles via SSH

Configuration profiles can also be loaded to the TAINY xMOD and activated with the SSH access (see chapter 8.2).

To do this, copy the configuration profile (e.g. TAINY.tgz) via SSH to the directory /webserver/profiles/.

Then copy a trigger file with the following name to the same directory:

<Configuration-profile>@now.trigger

As soon as the TAINY xMOD recognises this file in the directory, the new configuration profile is adopted. It makes no difference what the contents of the trigger file are.

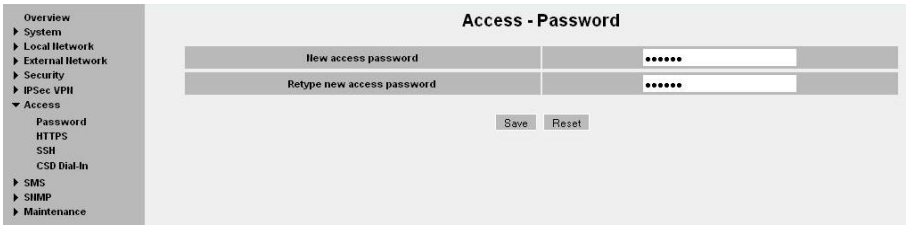
Example:

Configuration profile: TAINY.tgz

Trigger file: TAINY.tgz@now.trigger

3.8 Changing the password

Access > Password



Function

Access to the TAINY xMOD is protected by an access password. This access password protects access by way of both the

- local interface to the Web user interface, and
- local interface to the SSH console,

as well as the access to the available wireless connection (HDSPA, UMTS, EGPRS or GPRS)

- UMTS/GPRS by https to the Web user interface, and
- UMTS/GPRS to the SSH console

Access password (factory setting)

The factory setting for the TAINY xMOD is:

- Password: *root*
- User name: *root (*cannot be changed)

Note

Please change the password immediately after initial start-up. The factory setting is general knowledge and does not provide sufficient protection.

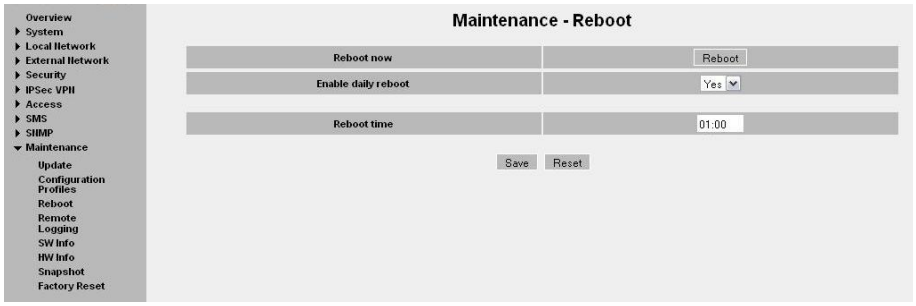
New access password (with confirmation)

To change the password, enter the new password you have selected in *New access password* and confirm the entry in *Retype new access password.*

Reset can be used to discard any entries that have not yet been saved. *Save* accepts the new password.

3.9 Reboot

Maintenance > Reboot



Function

Although the TAINY xMOD is designed for continuous operation, in such a complex system faults may occur, often triggered by external influences. A reboot can rectify these faults.

The reboot resets the functions of the TAINY xMOD. Current settings according to the configuration profile do not change. The TAINY xMOD continues to work using these settings after the reboot.

Reboot now

The reboot is carried out immediately when you click on *Reboot*.

Enable daily reboot

The reboot is carried out automatically once a day if you switch the function on with *Yes*.

Specify the *Time of the daily reboot*. The reboot will be carried out at the specified system time. Existing connections will be interrupted.

Factory setting

Enable daily reboot: **No**

Reboot time **01:00**

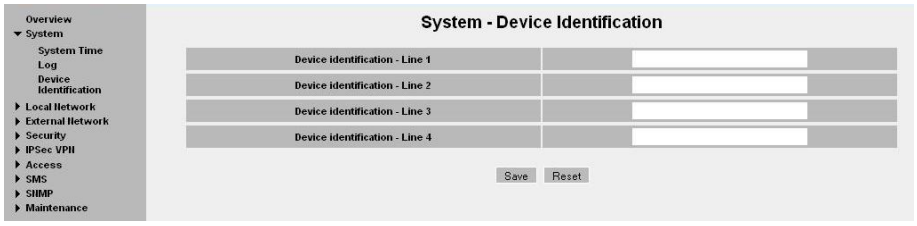
3.10 Load factory settings

Maintenance > Factory Reset

Reset to factory settings	A click on the push button *Reset* loads the factory settings, resets the passwords and deletes the stored certificates, the configuration profiles and the archived log files. The TAINY HMOD-V2-IO and the TAINY EMOD-V2-IO will also delete the saved certificate.
Service button	The load of the factory settings can also be activated by pushing the service button (see chapter 2.4).
Default configuration	If you only intend to load the factory settings without deleting the configuration profiles and archived logs, then only activate the standard configuration as described in chapter 3.7.This process also applies to the certificates for the TAINY HMOD-V2-IO and the TAINY EMOD-V2-IO.

3.11 Device identification

System – Device identification

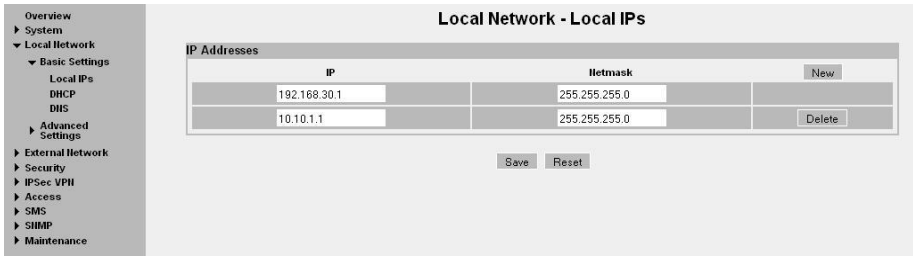


Device identification – Line 1 - 4	The TAINY xMOD provides four text fields in which the desired strings can be saved, for such purposes as device identification. The text fields can be written in and read. The text fields are each limited to 60 characters.
Character set	! $ % & ' ( ) * + , . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ _ ` a b c d e f g h I j k l m n o p q r s t u v w x y z { | }
SNMP	The four text fields can be read via SNMP (see chapter 11.1)

4 Local interface

4.1 IP addresses of the local interface

Local Network > Basic Settings > Local IPs

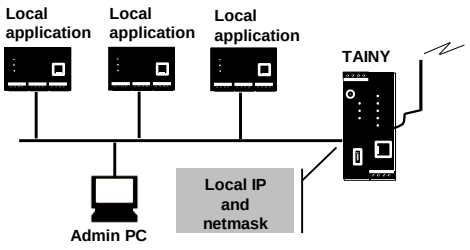


Local IP address acc. to factory setting:
192.168.1.1

This is where the IP addresses and the net masks at which the TAINY xMOD can be reached by local applications are set. The factory settings for the TAINY xMOD are as follows:

IP	192.168.1.1
Netmask	255.255.255.0

These factory-set IP addresses and net masks can be changed freely, but should follow the applicable recommendations (RFC 1918).



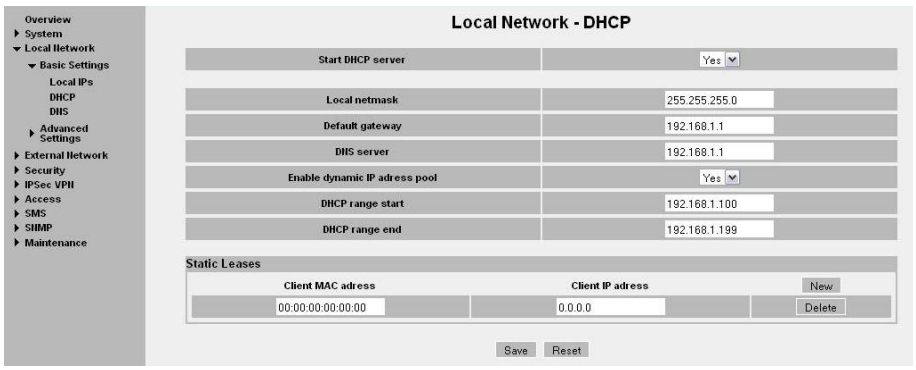
You can define additional addresses at which the TAINY xMOD can be reached by local applications. This is useful, for example, when the local network is subdivided into subnetworks. Then multiple local applications from different subnetworks can reach TAINY xMOD under various addresses.

New Adds additional IP addresses and net masks, which you can then modify in turn.

Delete Removes the respective IP address and netmask. The first entry cannot be deleted.

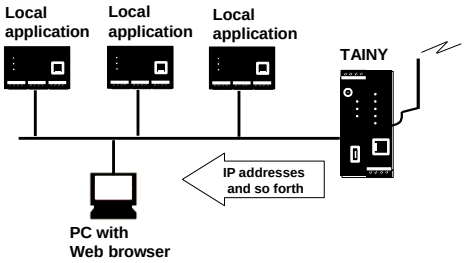
4.2 DHCP server to local network

Local Network > Basic Settings > DHCP



DHCP function

The TAINY xMOD contains a DHCP server (DHCP = Dynamic Host Configuration Protocol). If the DHCP server is switched on, it automatically assigns to the applications that are connected to the local interface of the TAINY xMOD the IP addresses, net masks, the gateway and the DNS server. This is only possible the setting for obtaining the IP address and the configuration parameter automatically via DHCP is activated for the local applications.



Start DHCP server

Start DHCP server – *Yes* switches on the DHCP server of the TAINY xMOD; *No* switches it off.

Local netmask

Here enter the local netmask that should be assigned to the local applications.

Default gateway

Here enter the default gateway that should be assigned to the local applications.

DNS server

Here enter the DNS server that should be assigned to the local applications.

Enable dynamic IP address pool

With *Yes* the IO addresses that the DHCP server of the TAINY xMOD assigns are drawn from a dynamic address pool.

With *No* the IP addresses must be assigned to the MAC addresses of the local application under *Static Leases*.

DHCP range start

Specifies the first address of the dynamic address pool.

DHCP range end

Specifies the last address of the dynamic address pool.

Static Leases

In Static Leases of the IP addresses you can assign corresponding IP addresses to the MAC addresses of local applications.

If a local application requests assignment of an IP address via DHCP, the application communicates its MAC address with the DHCP query. If an IP address is statically assigned to this MAC address the TAINY xMOD assigns the corresponding IP address to the application.

MAC address of the client –

MAC address of the querying local application

IP address of the client –

assigned IP address

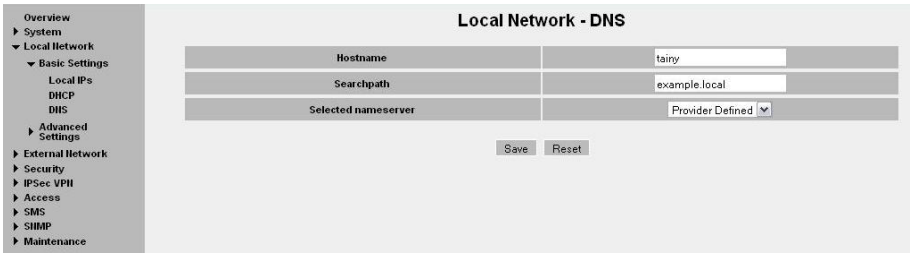
Factory setting

The factory settings for the TAINY xMOD are as follows:

Start DHCP server	**No**
Local netmask	**255.255.255.0**
Default gateway	**192.168.1.1**
DNS server	**192.168.1.1**
Enable dynamic IP address pool	**No**
DHCP range start	**192.168.1.100**
DHCP range end	**192.168.1.199**

4.3 DNS to local network

Local Network > Basic Settings > DNS

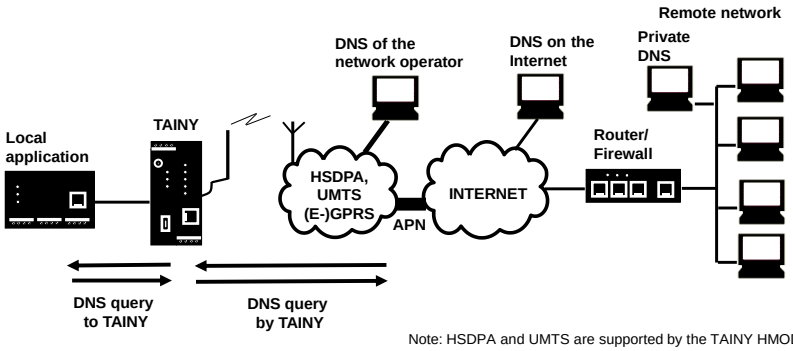


DNS function

The TAINY xMOD provides a domain name server (DNS) to the local network.

If you enter the IP address of the TAINY xMOD in your local application as the domain name server (DNS), then the TAINY xMOD answers the DNS queries from its cache. If it does not know the corresponding IP address for a domain address, then the TAINY xMOD forwards the query to an external domain name server (DNS).

The time period for which the TAINY xMOD holds a domain address in the cache depends on the host being addressed. In addition to the IP address, a DNS query to an external domain name server also supplies the life span of this information.



Note: HSDPA and UMTS are supported by the TAINY HMOD only.

The external domain name server (DNS) used can be a server of the network operator, a server on the Internet, or a server in a private external network.

Selected nameserver

Select which domain name server (DNS) the TAINY xMOD should query.

Provider Defined	When a connection is established to UMTS/GPRS the network operator automatically communicates one or more DNS addresses. These are then used.
User Defined	As the user you select your preferred DNS. The DNSes can be connected to the Internet, or it can be a private DNS in your network.

User defined nameserver

If you have selected the option *User Defined* then please enter the IP address of the selected DNS as the *Server IP Address*.

New can be used to add additional DNSes.

Factory setting

The factory settings for the TAINY xMOD are as follows:

Selected nameserver	**Provider Defined**
User defined nameserver	**-**
for new entry	**0.0.0.0**

4.4 Local hostname

Local Network > Basic Settings > DNS

The TAINY xMOD can also be addressed from the local network using a host name. To do this, define a host name, e.g. *myTAINY*.

The TAINY xMOD can then be called up, for example from a Web browser as *myTAINY*.

Note

The security concept of the TAINY xMOD requires the creation of an outgoing firewall rule for each local application that is to use this hostname function. See Chapter 6.1.

If you do not use DHCP (see Chapter 4.2), then identical search paths have to be entered manually in the TAINY xMOD and in the local applications. If you do use DHCP, the local applications received the search path entered in the TAINY xMOD via DHCP.

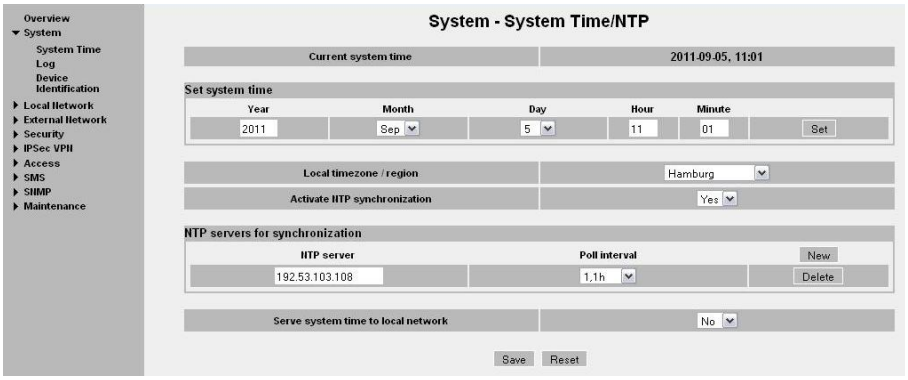
Factory setting

The factory settings for the TAINY xMOD are as follows:

Searchpath	**example.local**
Hostname	**tainy**

4.5 System Time/NTP

System > System Time



Setting the system time manually

This is where you set the system time for the TAINY xMOD. This system time is:

- used as a time stamp for all log entries, and
- serves as a time basis for all time-controlled functions.

Select the year, month, day, hour and minute.

Activate NTP synchronization

The TAINY xMOD can also obtain the system time from a time server via NTP (= *Network Time Protocol*). There are a number of time servers on the Internet that can be used to obtain the current time very precisely via NTP.

Local timezone / region

The NTP time servers communicate the UTC (= *Universal Time Coordinated*). To specify the time zone, select a city near the location near where the TAINY xMOD will be operating. The time in this time zone will then be used as the system time.

NTP server

Click on *New* to add an NTP server, and enter the IP address of such an NTP server, or use the NTP server factory preset. You can specify multiple NTP servers at the same time.

It is not possible to enter the NTP address as a hostname (e.g. timeserver.org).

Poll interval

The time synchronization is carried out cyclically. The interval at which synchronization is performed is determined by the TAINY xMOD automatically. A new synchronisation will be carried out at least once every 36 hours. The poll interval defines the minimum period that the TAINY xMOD waits until the next synchronization.

Note

Synchronising the system time via NTP causes additional data traffic on the wireless data connection. Depending on the selected settings, the additional data traffic can amount to 120 Kbyte per month or more. This entails higher costs, depending on the participant contract with the GSM network operator.

Serve system time to local network

The TAINY xMOD can serve itself as an NTP time server for the applications that are connected to its local network interface. To activate this function select *Yes*.

The NTP time server in the TAINY xMOD can be reached via the local IP address set for the TAINY xMOD, see Chapter 4.1.

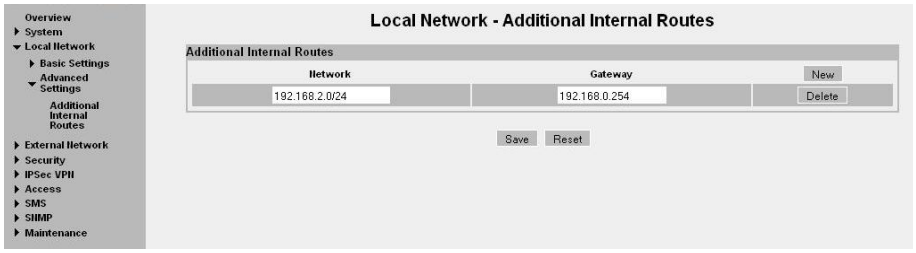
Factory setting

The factory settings for the TAINY xMOD are as follows:

Local timezone	**UTC**
Activate NTP synchronization	**No**
NTP server	**192.53.103.108**
Poll interval	**1.1 hours**
Serve system time to local network	**No**

4.6 Additional Internal Routes

Local Network > Advanced Settings > Additional Internal Routes



Function

If the local network is subdivided into subnetworks, you can defines additional routes.

See also Chapter 11.

To define an additional route to a subnetwork, click on *New*.
Specify the following:
- the IP address of the subnetwork (network), and also
- the IP address of the gateway via which the subnet is connected.

You can define any desired number of internal routes.

To delete an internal route, click on *Delete*.

Factory setting

The factory settings for the TAINY xMOD are as follows:

Additional Internal Routes **-**

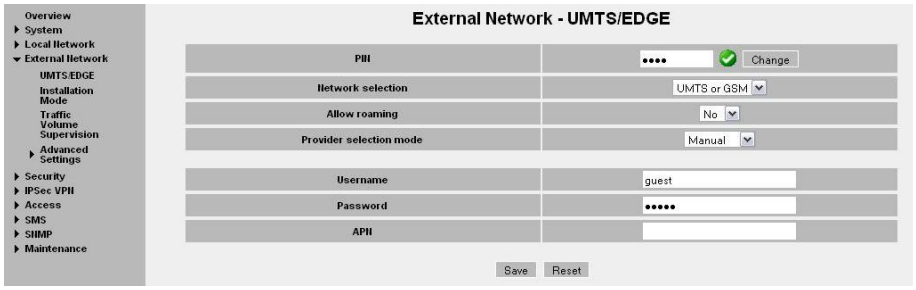
Default for new routes:

Network:	**192.168.2.0/24**
Gateway:	**192.168.0.254**

5 External interface

5.1 Network selection and access parameters for UMTS/GPRS

External Network > UMTS/EDGE

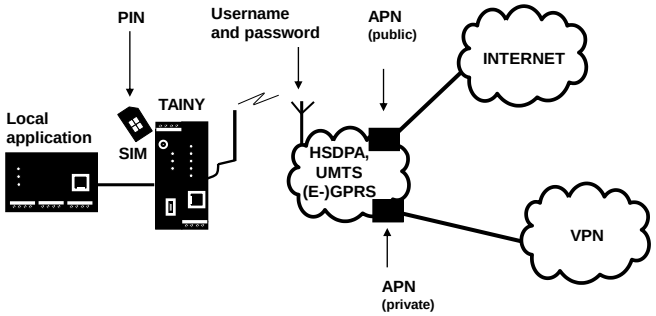


Function

The TAINY HMOD uses HSDPA, UMTS data, EGPRS or GPRS as the mobile data service for communication with the external network. The type of mobile communications network (UMTS or GSM) must be selected.

The TAINY EMOD uses EGPRS or GPRS as a mobile data service. Access parameters which you receive from your wireless network operator are required for access to these IP wireless network services and to the basic wireless network.

The PIN protects the SIM card against unauthorised use. The user name and password protect the access to the mobile radio services and the APN (Access Point Name) defines the transition from the mobile radio services to additional connected IP networks, for example a public APN to the Internet or a private APN to a virtual private network (VPN).



Note: HSDPA and UMTS are supported by the TAINY HMOD only.

Network selection

ONLY TAINY HMOD

The TAINY HMOD can be connected to the UMTS or GSM mobile communications networks at your discretion.

- UMTS (with the services UMTS data and HSDPA)
- GSM (with the services EGPRS, GPRS and CSD

With the setting *UMTS or GSM*, the TAINY HMOD preferentially selects a UMTS network depending on availability. If this is unavailable, a GSM network will be used.

With the setting *GSM only*, the TAINY HMOD selects a GSM network in any case.

Allow roaming

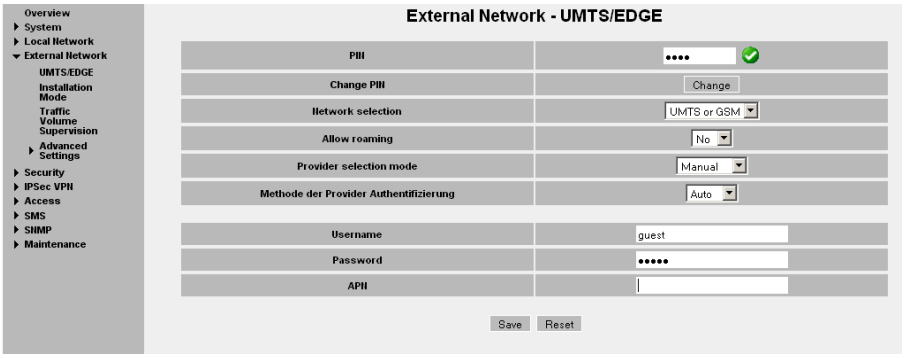
Select *No* if the TAINY xMOD should exclusively be logged into the home network (mobile communications network) whose SIM card is inserted.

Select *Yes* if the TAINY xMOD may also be logged into partner networks of the home network if the home network cannot be reached or only with poor connectivity.

Warning

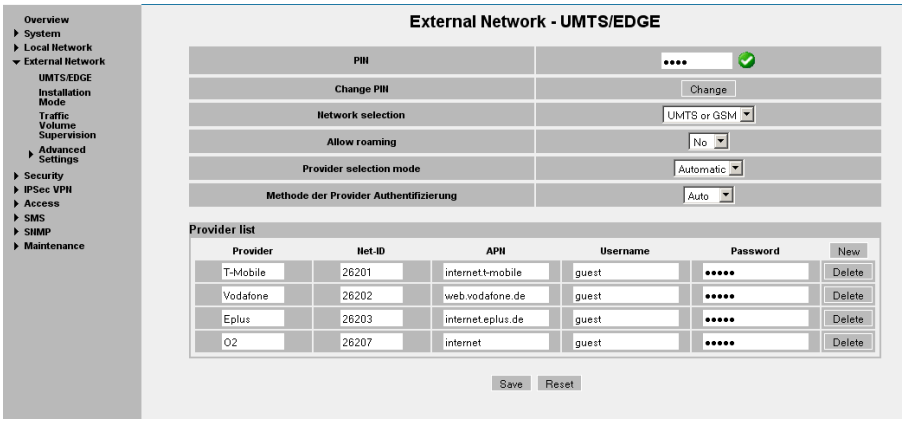
Considerable additional costs may be incurred if the TAINY xMOD logs into a partner network (roaming).

Provider selection mode - Manual



If the Provider selection mode Manual is active, enter the Username, the Password and the APN for UMTS, EGPRS or GPRS manually.

Provider selection mode - Automatic



If the Provider selection mode Automatic is active, the access data for UMTS, EGPRS or GPRS are selected automatically. The access data will be selected depending on the Net-ID of the SIM carder from the provider list. Several entries can be inserted in the provider list. The quantity is not limited, but more than 10 entries should be avoided.

Click on New to insert a new entry. Click on Delete to remove entries.

PIN

Enter the PIN for your SIM card here. You will receive the PIN from your network operator.

The TAINY xMOD also works with SIM cards that have no PIN; in this case please enter ***NONE***. In this case the input box is left empty.

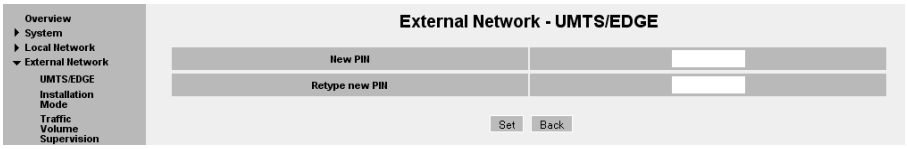
Note

If no entry is made, the input box for the PIN is shown with a red outline after saving.

Change PIN

Press the *Change* button to change the PIN on the SIM card.

A submenu opens.



New PIN — Enter the new PIN here.

New PIN (repeated) — Enter the new PIN again to confirm.

Note

If the PIN query is deactivated with the SIM card inserted (PIN-less card), then the PIN cannot be activated or changed.

Provider (only in case of provider selection mode Automatic) — Enter as free text the description of the UMTS or GPRS service, e.g. the Provider name (e.g. Vodafone, Eplus, my GPRS access).

Net-ID (only in case of provider selection mode Automatic) — Enter the identification number of the network provider to which the UMTS or GPRS access data of the same line of the provider list are related to.

Each UMTS or GSM/GPRS network has a worldwide unique identification number. This number is stored on the SIM card. The TAINY xMOD reads this Net-ID from the SIM card and selects the corresponding GPRS access data from the provider list.

You find the NET-ID at our Web site www.neuhaus.de, in the information documents of your UMTS or GSM/GPRS provider, at his homepage or you can ask the hotline of the provider (keyword: MCC/MNC).

User name — Enter the user name for the UMTS/GPRS here. Some mobile radio network operators do not use access control with user names and/or passwords. In this case enter *guest* in the corresponding box.

Password — Enter the password for UMTS/GPRS here. Some mobile radio network operators do not use access control with user names and/or passwords. In this case enter *guest* in the corresponding box.

APN — Enter the name of the transition from UMTS/GPRS to other networks here.

You can find the APN in your mobile radio network operator's documentation, on your operator's Website, or ask your operator's hotline.

Method of provider Authentication — For registration at the wireless data service (HSDPA, UMTS, EGPRS or GPRS), two different methods (PAP and CHAP) are used. In general, the selection of the method is performed automatically. If a particular method shall be used, the selection may be done manually. Choose from Auto, PAP or CHAP.

Factory setting

The factory settings for the TAINY xMOD are as follows:

Only TAINY HMOD-V2-IO

Network selection	**UMTS or GSM**
Mode of provider selection	**Automatic**
Roaming	**No**

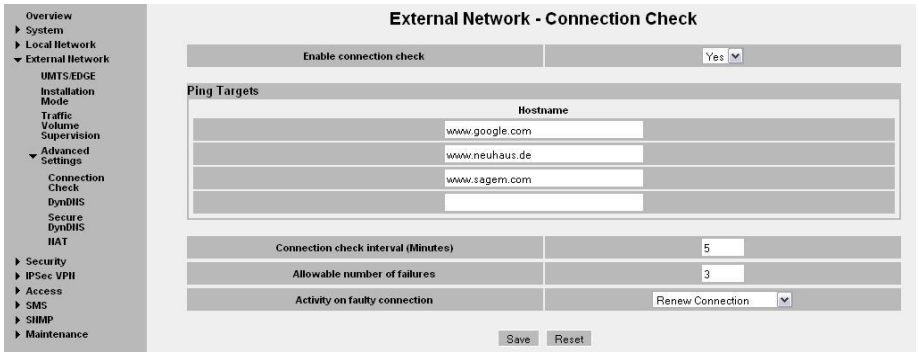
Provider selection mode - Manual

PIN	**NONE**
Username	**guest**
Password	**guest**

	APN	**NONE**
Provider selection mode - Automatic	1. Provider	**T-Mobile**
	Net-ID	**26201**
	Username	**guest**
	Password	**guest**
	APN	**internet.t-mobile**
	2. Provider	**Vodafone**
	Net-ID	**26202**
	Username	**guest**
	Password	**guest**
	APN	**web.vodafone.de**
	3. Provider	**Eplus**
	Net-ID	**26203**
	Username	**guest**
	Password	**guest**
	APN	**internet.eplus.de**
	4. Provider	**O2**
	Net-ID	**26207**
	Username	**guest**
	Password	**guest**
	APN	**internet**
	n. Provider	**NONE**
	Net-ID	**NONE**
	Username	**NONE**
	Password	**NONE**
	APN	**NONE**
	Method of provider authentication	**Auto**

5.2 UMTS/GPRS connection monitoring

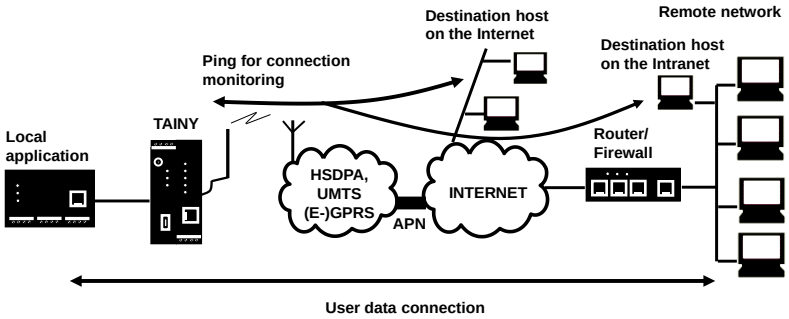
External Network > Advanced Settings > Connection Check



Function

With the function *Connection Check* the TAINY xMOD checks its connection to UMTS/GPRS and to the connected external networks, such as the internet or an intranet. To do this, the TAINY xMOD sends ping packets (ICMPs) to up to four remote stations (target hosts) at regular intervals. This takes place independently of the user data connections. If after such a ping the TAINY xMOD receives a response from at least one of the remote stations addressed, then the TAINY xMOD is still connected with the UMTS/GPRS and ready for operation.

Some *network operators* interrupt connections when they are inactive. This is likewise prevented by the *Connection Check* function.



Note: HSDPA and UMTS are supported by the TAINY HMOD only.

Warning

Sending ping packets (ICMPs) increases the amount of data sent and received via the UMTS/GPRS. The additional data traffic can add up to 2.5 Mbyte per month (ping to IP address) or 6 Mbyte per month (Ping to hostname), depending on the settings selected. This can lead to increased costs.

Enable connection check *Yes* activates the function.

Ping Targets - Hostname Select up to four remote stations that the TAINY xMOD can ping. The remote stations must be available continuously and must answer pings.

Note

Make sure that the selected remote stations will not feel "harassed".

Connection check interval (minutes) Specifies the interval at which the connection check ping packets are sent by the TAINY xMOD. This is specified in minutes.

Allowable number of failures Specifies how many times it is allowed for all ping packets of an interval not to receive an answer, i.e. for none of four pinged remote stations to answer, before the specified action is carried out.

Activity on faulty connection	*Renew Connection*	The TAINY xMOD re-establishes the connection to the UMTS/GPRS if the ping packets sent were not answered.
	Reboot TAINY xMOD	The TAINY xMOD carries out a reboot if the ping packets sent were not answered.

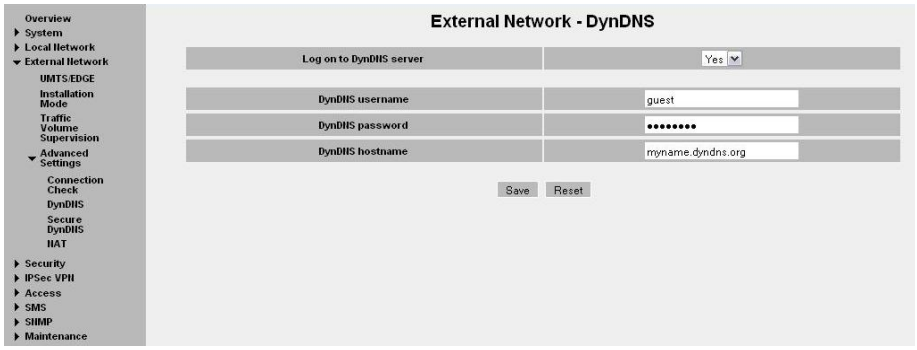
Factory setting

The factory settings for the TAINY xMOD are as follows:

Enable connection check	**No (switched off)**
Hostname	**-**
Connection check interval	**5 (minutes)**
Allowable number of failures	**3 (failed attempts)**
Activity on faulty connection	**Renew Connection**

5.3 Hostname via DynDNS

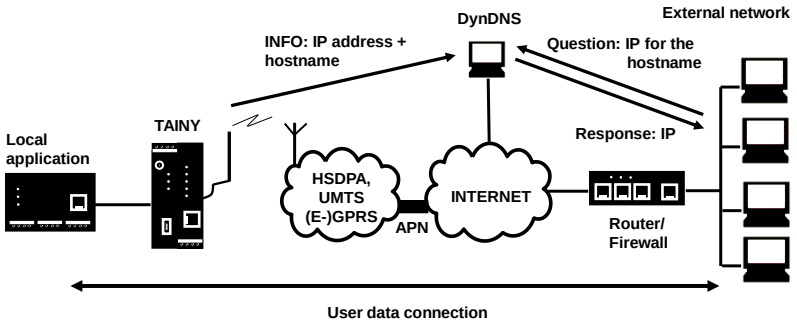
External Network > Advanced Settings > DynDNS



Function

Dynamic domain name servers (DynDNS) make it possible for applications to be accessible on the Internet under a hostname (e.g. myHost.org), even if these applications do not have a fixed IP address and the hostname is not registered. If you log the TAINY xMOD on to a DynDNS service, you also can reach the TAINY xMOD from external network under a hostname, e.g. myTainy.dyndns.org.

For more information on DynDNS see Chapter 11.



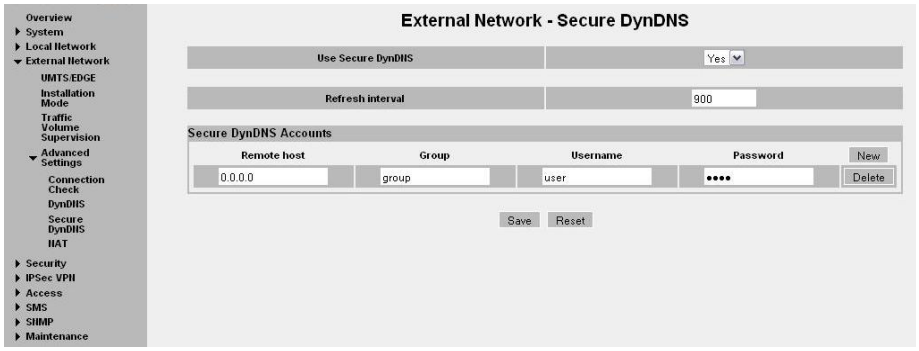
Note: HSDPA and UMTS are supported by the TAINY HMOD only.

Log this TAINY on to a DynDNS server	Select *Yes* if you want to use a DynDNS service.
Log on interval (seconds)	The TAINY xMOD is compatible with dyndns.org.
DynDNS username / password	Enter here the username and the password that authorise you to use the DynDNS service. Your DynDNS provider will give you this information.

DynDNS hostname	Here enter the hostname that you have agreed with your DynDNS provider for the TAINY xMOD, e.g. myTAINY.dyndns.org.
DynDNS provider	The TAINY xMOD is compatible to dyndns.org
Factory setting	The factory settings for the TAINY HMOD-V2-IO are as follows:
	Log the TAINY on to DynDNS server **No (switched off)**
	DynDNS username **guest**
	DynDNS password **guest**
	DynDNS hostname **myname.dyndns.org**

5.4 Secure DynDNS

External Network > Secure DynDNS

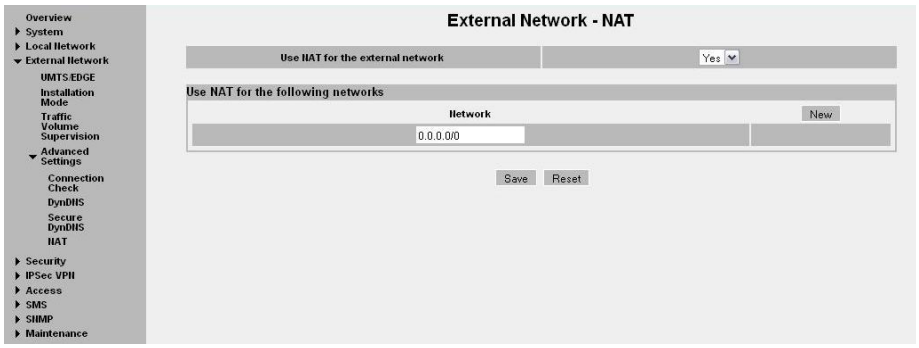


Function	With Siemens Remote Service being activated, the TAINY xMOD transmits its external IP address being assigned by the EDGE/GPRS service via secured https protocol to a selectable remote host. This function is comparable to DynDNS service and requires an applicable access point at the host side.
Use Siemens Remote Service	Click *Yes*, if you like to use the Siemens Remote Service. Click *New* to add additional remote hosts, click *Delete* to remove existing entries.
Refresh interval	Enter the interval in seconds, applied to transmit periodically the IP address of the TAINY xMOD to the remote host.
Secure DynDNS Accounts	Enter the target IP address and the access data of one or more remote hosts. **Remote host** Enter the target IP address of the remote host. **Group** Enter the group information. **Username** Enter the Username to access the remote host. **Password** Enter the Password to access the remote host.
Factory setting	The factory settings for the TAINY xMOD are as follows:
	Use Secure DynDNS Accounts No (switched off)
	Refresh interval 900 seconds

Remote host	0.0.0.0
Group	group
Username	user
Password	pass

5.5 NAT – Network Address Translation

External network > NAT



Function

This lists the fixed rules for NAT (**N**etwork **A**ddress **T**ranslation) and allows rules to be set or deleted.

For outgoing data packets the TAINY xMOD can translate the given sender IP addresses from its internal network to its own external address, a technique known as NAT (Network Address Translation).

This method is used when the internal addresses cannot or should not be routed, e.g. because a private address range such as 192.168.x.x or the internal network structure is to be hidden.

This method is also called *IP Masquerading*.

Use NAT for the external network

Select *Yes* if you want to use the NAT function.

Use NAT for the following networks

Enter the network to which NAT shall be applied to. To denote a range, use CIDR syntax.

New – Add a network

Delete – Delete a network

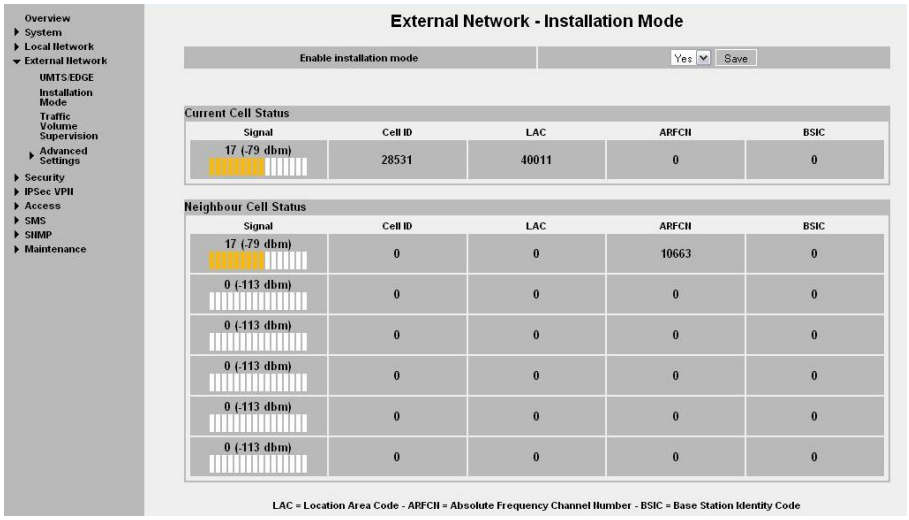
Factory setting

The factory settings for the TAINY HMOD-V2-IO are as follows:

Use NAT for the external network	**Yes (switched on)**
Network	**0.0.0.0/0**.

5.6 Installation mode

External network - Installation mode



Installation mode supports the positioning of the antenna and provides information about the cells in the surrounding area. If installation mode is activated, the signal strengths and additional characteristics of the cells in the surrounding area will be updated every three seconds.

Similarly, the display of the indicator lamp Q (Quality) is updated every three seconds in installation mode. In normal operation with a connection established, the query for this data takes place at 60 second intervals.

The position of the antenna should be changed until the displayed signal of the current cell has reached a maximum.

Activate installation mode	Select *Yes* in order to switch on installation mode. Select *No* to switch off installation mode and return to normal operation.

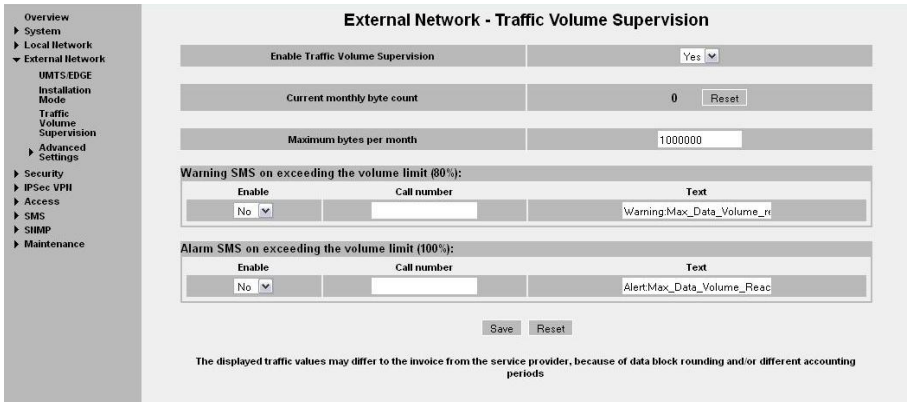
Attention

All connections to the external network are disconnected in installation mode. Normal live operation is not possible in installation mode.

Current Cell Status	Shows the characteristics of the cell to which the TAINY xMOD is currently connected.
Neighbour Cell Status	Shows the characteristics of neighbour cells from which the TAINY xMOD receives signals.
Signal	Display of the quality/field strength with which the signal of the cell is received. The CSQ value is specified and converted as an RSSI value [dBm].
Cell ID	Specifies the identification (Cell ID) of the cell.
LAC	Specifies the identification (LAC) of the network section comprised of multiple base stations / cells in the vicinity of the TAINY xMOD.
ARFCN	Indicates the number (ARFCN) of the radio channel on which the cell broadcasts.
BSIC	Specifies the identification (BSIC) of the base station to which the cell belongs.

5.7 Volume supervision

External network – Volume monitoring



Considerable additional costs may be incurred if the amount of data sent and received by the TAINY xMOD exceeds the data volume agreed upon with the wireless network operator.

Therefore, it may be beneficial if the data volume the TAINY xMOD uses is monitored and a warning is issued when a variable limit value is approached.

Enable Traffic Volume Supervision	Select *Yes* in order to switch on the traffic volume supervision. Select *No* in order to switch off the traffic volume supervision.
Current monthly byte count	Shows the number of bytes sent and received since the beginning of the month.

Note

Manually set the system time of the TAINY xMOD or activate the NTP synchronization, see chapter 4.5.

Reset	Press the button if you want to reset the counter for the bytes sent and received to 0. This takes place automatically at the end of the month.
Maximum bytes per month	Enter the limit value for the monthly data volume in bytes here.
Warning SMS on exceeding the volume limit (80%)	Select *Yes* if you want the TAINY xMOD to send an SMS with a warning message to the specified call number upon reaching 80% of the maximum data volume.
Alarm SMS on exceeding the volume limit (100%)	Select *Yes* if you want the TAINY xMOD to send an SMS with an alert message to the specified call number upon reaching the maximum data volume.
Call number	Enter the mobile call number which the SMS with the alarm or warning message should be sent to here.
Text	Enter the text of the alarm or warning SMS here.

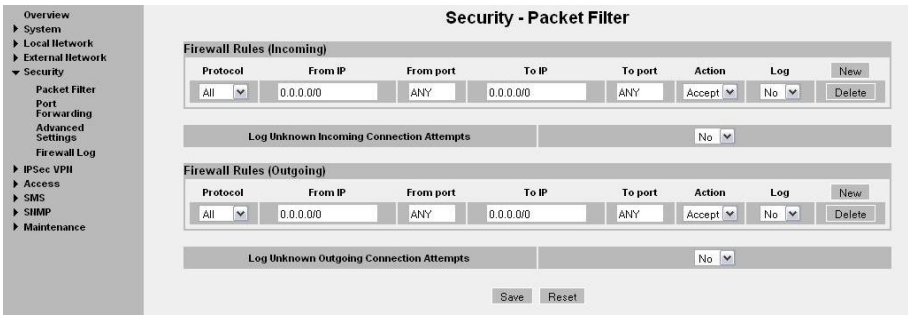
Note

The data volume detected only serves as an indication and may deviate from the calculation of the GSM network operator.

6 Security functions

6.1 Packet Filter

Security > Packet Filter



Function

The TAINY xMOD contains a stateful inspection firewall.

A stateful inspection firewall is a packet filtering method. Packet filters only let IP packets through if this has been defined previously using firewall rules. The following is defined in the firewall rules:

- which protocol (TCP, UDP, ICMP) can go through,
- the permitted source of the IP packets (From IP / From port)
- the permitted destination of the IP packets (To IP / To port)

It is likewise defined here what will be done with IP packets that are not allowed through (discard, reject).

For a simple packet filter it is always necessary to create two firewall rules for a connection:

- One rule for the query direction from the source to the destination, and
- a second rule for the query direction from the destination to the source.

It is different for a TAINY xMOD with a stateful inspection firewall. Here a firewall rule is only created for the query direction from the source to the destination. The firewall rule for the response direction from the destination to the source results from analysis of the data previously sent. The firewall rule for the responses is closed again after the responses are received or after a short time period has elapsed. Thus responses can only go through if there was a previous query. This means that the response rule cannot be used for unauthorised access. What is more, special procedures make it possible for UDP and ICMP data to also go through, even though these data were not requested before.

Firewall Rules (Incoming)

The Firewall Rules (Incoming) are used to define how to handle IP packets that are received from external networks (e.g. the Internet) via UMTS/GPRS. The source is the sender of this IP packet. The destination is the local applications on the TAINY xMOD.

In the factory setting, no incoming firewall rule is set initially, i.e. no IP packets can go through.

New Adds an additional firewall rule that you can then fill out.

Delete Removes firewall rules that have been created.

Protocol Select the protocol for which this rule will be valid. The following selections are available: *TCP, UDP, ICMP*. If you select *All*, the rule is valid for all three protocols.

Note

If you select *All for* protocol, a port assignment is not effective.

From IP Enter the IP address of the external remote station that is allowed to send IP packets to the local network. Do this by specifying the IP address or an IP range for the remote station. ***0.0.0.0/0*** means all addresses.

To specify a range, use the CIDR notation - see Chapter 11.

From port Enter the port from which the external remote station is allowed to send IP packets.

(is only evaluated for the protocols TCP and UDP)

To IP Enter the IP address in the local network to which IP packets may be sent. Do this by specifying the IP address or an IP range of the application in the local network. ***0.0.0.0/0*** means all addresses.

To specify a range, use the CIDR notation - see Chapter 11.

To port Enter the port to which the external remote station is allowed to send IP packets.

Action Select how incoming IP packets are to be handled:

Accept – The data packets can go through,

Reject – The data packets are rejected, and the sender receives a corresponding message.

Drop – The data packets are discarded without any feedback to the sender.

Firewall Rules (Outgoing) The Firewall Rules (Outgoing) are used to define how to handle IP packets that are received from the local network. The source is an application in the local network. The destination is an external remote station, e.g. on the Internet or in a private network.

In the factory setting, no outgoing firewall rule is set initially, i.e. no IP packets can go through.

New Adds an additional firewall rule that you can then fill out.

Protocol Select the protocol for which this rule will be valid. The following selections are available: *TCP, UDP, ICMP*. If you select *All*, the rule is valid for all three protocols.

From IP Enter the IP address of the local application that is allowed to send IP packets to the external network. Do this by specifying the IP address or an IP range for the local application. ***0.0.0.0/0*** means all addresses.

To specify a range, use the CIDR notation - see Chapter 11.

From port Enter the port from which the local network is allowed to send IP packets. Do this by specifying the port number.

(is only evaluated for the protocols TCP and UDP)

To IP Enter the IP address in the external network to which IP packets may be sent. Do this by specifying the IP address or an IP range of the application in the network. ***0.0.0.0/0*** means all addresses.

To specify a range, use the CIDR notation - see Chapter 11.

	To port	Enter the port to which the external local application is allowed to send IP packets. Do this by specifying the port number. (is only evaluated for the protocols TCP and UDP)
	Action	Select how outgoing IP packets are to be handled: Accept – The data packets can go through, Reject – The data packets are rejected, and the sender receives a corresponding message. Drop – The data packets are discarded without any feedback to the sender.
Firewall Rules Incoming / Outgoing	*Log*	For each individual firewall rule you can define whether the event should be □ logged when the rule takes effect - set *Log* to *Yes* □ or not - set *Log* to *No* (factory setting) The log is kept in the firewall log, see Chapter 6.4.
Log Unknown Connection Attempts	This logs all connection attempts that are not covered by the defined rules.	

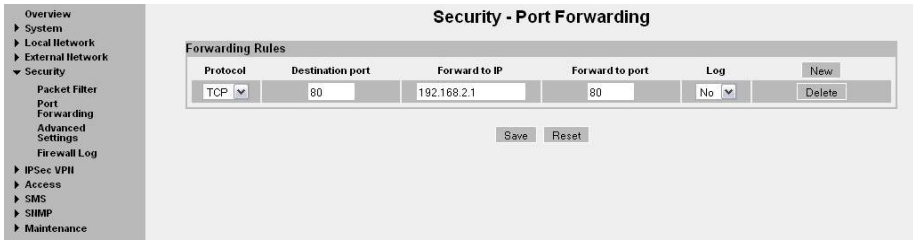
Factory setting

The factory settings for the TAINY xMOD are as follows:

Incoming firewall	Firewall Rules (Incoming)	**- (Everything blocked)**
	Protocol	**All**
	From IP	**0.0.0.0/0**
	From port	**Any**
	To IP	**0.0.0.0/0**
	To port	**Any**
	Action	**Accept**
	Log	**No (switched off)**
	Log Unknown Connection Attempts	**No (switched off)**
Outgoing firewall	Firewall Rules (Outgoing)	**- (Everything blocked)**
	Protocol	**All**
	From IP	**0.0.0.0/0**
	From port	**Any**
	To IP	**0.0.0.0/0**
	To port	**Any**
	Action	**Accept**
	Log	**No (switched off)**
	Log Unknown Connection Attempts	**No (switched off)**

6.2 Port Forwarding

Security > Port Forwarding



Function

If a rule has been created for port forwarding, then data packets received at a defined IP port of the TAINY xMOD from the external network will be forwarded. The incoming data packets are then forwarded to a specified IP address and port number in the local network. The port forwarding can be configured for TCP or UDP.

In port forwarding the following occurs: The header of incoming data packets from the external network that are addressed to the external IP address of the TAINY xMOD and to a specific port are adapted so that they are forwarded to the internal network to a specific computer and to a specific port of that computer.
This means that the IP address and port number in the header of incoming data packets are modified.

This process is also called Destination NAT or Port Forwarding.

Note

In order for incoming data packets to be forwarded to the defined IP address in the local network, a corresponding incoming firewall rule must be set up for this IP address in the packet filter. See Chapter 6.1.

New	Adds a new forwarding rule that you can then fill out.
Delete	Removes forwarding rules that have been created.
Protocol	Specify here the protocol (TCP or UDP) to which the rule should refer.
Destination port	Specify here the port number (e.g. 80) at which the data packets which are to be forwarded arrive from the external network.
Forward to IP	Specify here the IP address in the local network to which the incoming data packets should be forwarded.
Forward to port	Specify here the port number (e.g.) for the IP address in the local network to which the incoming data packets should be forwarded.
Log	For each port forwarding rule you can define whether the event should be - logged when the rule takes effect - set *Log* to *Yes* - or not - set *Log* to *No* (factory setting) The log is kept in the firewall log, see Chapter 6.4.

Factory setting

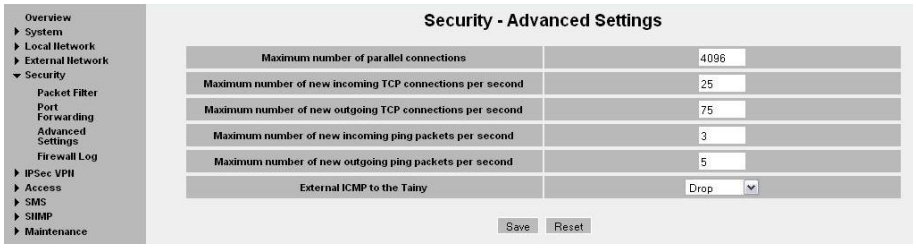
The factory settings for the TAINY xMOD are as follows:

Forwarding Rules	**-**
Protocol	**All**
Destination port	**80**

Forward to IP	**127.0.0.1**
Forward to port	**80**
Log	**No (switched off)**

6.3 Advanced security functions

Security > Advanced Settings



Function

The advanced security functions serve to protect the TAINY xMOD and the local applications against attacks. For protective purposes it is assumed that only a certain number of connections or received PING packets are permissible and desirable in normal operation, and that a sudden burst represents an attack.

Maximum number …

The entries

- Maximum number of parallel connections
- Maximum number of new incoming TCP connections per second
- Maximum number of new outgoing TCP connections per second
- Maximum number of new incoming ping packets per second
- Maximum number of new outgoing ping packets per second

set the upper limits. The settings (see illustration) have been selected so that they will in practice never be reached in normal use. In the event of an attack, however, they can be reached very easily, which means that the limitations constitute additional protection. If your operating environment contains special requirements, then you can change the values accordingly.

External ICMP to the TAINY

You can use this option to affect the response when ICMP packets are received that are sent from the external network in the direction of the TAINY xMOD. You have the following options:

- *Drop*: All ICMP packets to the TAINY xMOD are discarded.
- *Allow Ping*: Only ping packets (ICMP type 8) to the TAINY xMOD are accepted.
- *Accept*: All types of ICMP packets to the TAINY xMOD are accepted.

Factory setting

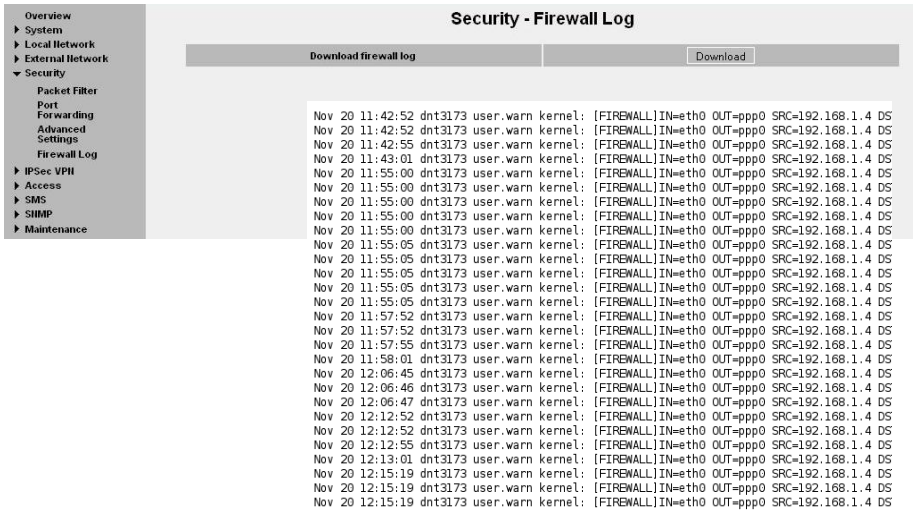
The factory settings for the TAINY xMOD are as follows:

Maximum number of parallel connections	**4096**
Maximum number of new incoming TCP connections per second	**25**
Maximum number of new outgoing TCP connections per second	**75**

Maximum number of new incoming ping packets per second	**3**
Maximum number of new outgoing ping packets per second	**5**
External ICMP to the TAINY	**Drop**

6.4 Firewall Log

Security > Firewall Log



Function

The application of individual firewall rules is recorded in the firewall log. To do this, the LOG function must be activated for the various firewall functions.

Caution

The firewall log is lost in the event of a reboot.

7 VPN connections

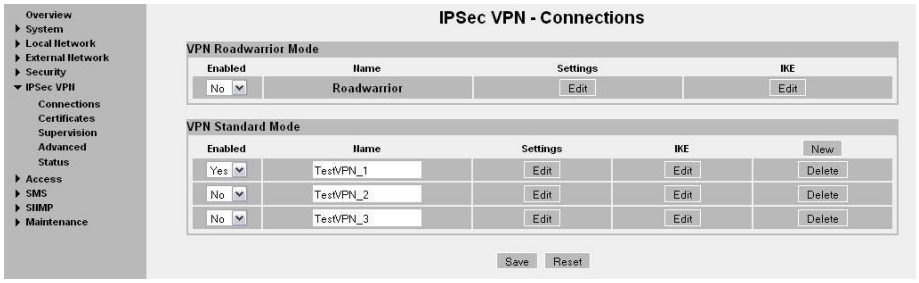
NUR TAINY HMOD-V2-IO
NUR TAINY EMOD-V2-IO

Note regarding the scope of function

The menu item IPsec-VPN is only present with the TAINY HMOD-V2-IO and TAINY EMOD-V2-IO. Only the TAINY HMOD-V2-IO and TAINY EMOD-V2-IO support IPsec-VPN connections.

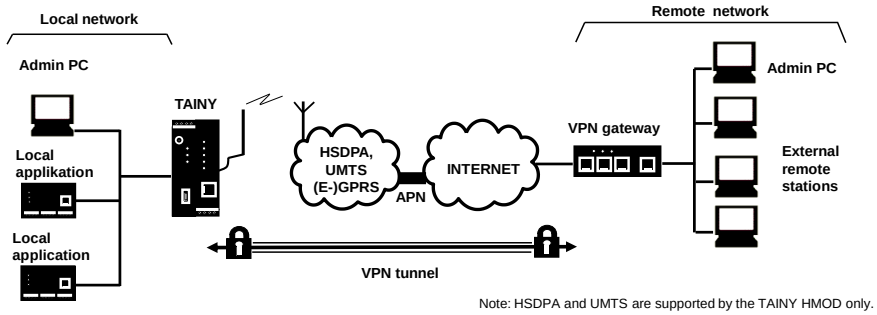
7.1 Introduction

IPsec VPN > Connections



Function

The TAINY xMOD-V2-IO can connect the local network to a friendly remote network via a VPN tunnel. The IP data packets that are exchanged between the two networks are encrypted, and are protected against unauthorised tampering by the VPN tunnel. This means that even unprotected public networks like the Internet can be used to transfer data without endangering the confidentiality or integrity of the data.



Note: HSDPA and UMTS are supported by the TAINY HMOD only.

For the TAINY xMOD-V2-IO to establish a VPN tunnel, the remote network must have a VPN gateway as the remote station for the TAINY xMOD-V2-IO

For the VPN tunnel, the TAINY xMOD-V2-IO uses the IPsec method in tunnel mode. In this method the IP data packets to be transmitted are completely encrypted and provided with a new header before they are sent to the remote station's VPN gateway. There the data packets are received, decrypted, and used to reconstruct the original data packets. These are then forwarded to their destination in the remote network.

Differences between two VPN connection modes:

- In VPN Roadwarrior Mode the TAINY xMOD-V2-IO VPN can accept connections from remote stations with an unknown address. These can be, for example, remote stations in mobile use that obtain their IP address dynamically.
  The VPN connection must be established by the remote station. Only one VPN connection is possible in Roadwarrior Mode. VPN connections in Standard Mode can be used at the same time.
- In VPN Standard Mode the address (IP address or hostname) of the remote station's VPN gateway must be known for the VPN connection to be established. The VPN connection can be established either by the TAINY xMOD-V2-IO or by the remote station's VPN gateway as desired.

Establishment of the VPN connection is subdivided into two phases: First in Phase 1 (ISAKMP = Internet Security Association and Key Management Protocol) the Security Association (SA) for the key exchange between the TAINY xMOD-V2-IO and the VPN gateway of the remote station is established.

After that in Phase 2 (IPsec = Internet Protocol Security) the Security Association (SA) for the actual IPsec connection between the TAINY xMOD-V2-IO and the remote station's VPN gateway is established.

Requirements for the remote network's VPN gateway

In order to successfully establish an IPsec connection, the VPN remote station must support IPsec with the following configuration:

- Authentication via X.509 certificates, CA certificates or pre-shared key (PSK)
- ESP
- Diffie-Hellman group 1, 2 or 5
- 3DES or AES encryption
- MD5 or SHA-1 hash algorithms
- Tunnel Mode
- Quick Mode
- Main Mode
- SA Lifetime (1 second to 24 hours)

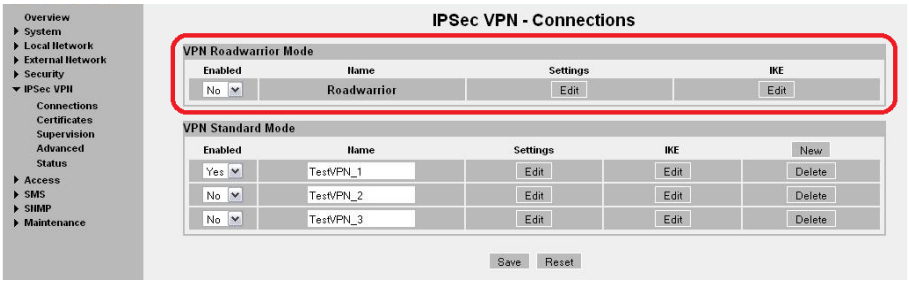
If the remote station is a computer running under Windows 2000, then the Microsoft Windows 2000 High Encryption Pack or at least Service Pack 2 must also be installed.

If the remote station is on the other side of a NAT router, then the remote station must support NAT-T. Or else the NAT router must know the IPsec protocol (IPsec/VPN passthrough).

7.2 VPN Roadwarrior Mode

IPsec VPN > Connections

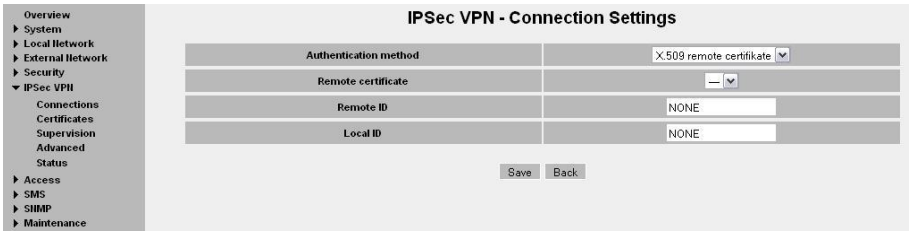
ONLY TAINY HMOD-V2-IO
ONLY TAINY EMOD-V2-IO



Function

The Roadwarrior Mode makes it possible for the TAINY xMOD-V2-IO VPN to accept a VPN connection initiated by a remote station with an unknown IP address. The remote station must authenticate itself properly; in this VPN connection there is no identification of the remote station based on the IP address or the hostname of the remote station.

Roadwarrior Mode Edit Settings



Function

Set the TAINY xMOD-V2-IO up in accordance with what has been agreed with the system administrator of the remote station.

Authentication method

Select the authentication method in accordance with what you have agreed with the system administrator of the remote station.

The TAINY xMOD-V2-IO supports three methods:

- X.509 certificate
- CA certificate
- Pre-shared key

X.509 certificate, CA certificate

In the authentication methods X.509 certificate and CA certificate, the keys used for authentication have first been signed by a Certification Authority (CA). This method is considered especially secure. A CA can be a service provider, but also, for example, the system administrator for your project, provided that he has the necessary software tools. The CA creates a certificate file (PKCS12) with the file extension *p12 for each of the two remote stations. This certificate file contains the public and private keys for the own station, the signed certificate from the CA, and the public key of the CA. For the authentication method X.509 there is additionally a key file (*.pem or *.crt) for each of the two remote stations with the public key of the own station.

X.509 certificate — The public keys (files with extension *.pem or *.crt) are exchanged between the TAINY xMOD-V2-IO and the remote station's VPN gateway takes place manually, for example on a CD-ROM or via e-mail. To load the certificate, proceed as described in Chapter 7.4.

CA certificate — The public keys are exchanged between the TAINY xMOD-V2-IO and the remote station's VPN gateway via the data connection when the VPN connection is established. Manual exchange of the key files is not necessary.

Pre-shared secret key (PSK)

This method is primarily supported by older IPsec implementations. Here authentication is performed with a character string agreed on beforehand. In order to obtain high security, the character string should consist of about randomly-selected 30 lower-case and upper-case letters and numerals.

The following characters are permitted:

! $ % & ' ( ) * + , . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ ` a b c d e f g h I j k l m n o p q r s t u v w x y z { | } #

Entered characters can not be read.

Remote certificate — If you have selected X.509 certificate as the authentication method, then a list of the remote certificates that you have already loaded into the TAINY xMOD-V2-IO is displayed here. Select the certificate for the VPN connection.

Remote ID

Local ID

The Local ID and the Remote ID are used by IPsec to identify the remote stations uniquely when establishing the VPN connection. The own Local ID constitutes the Remote ID of the remote station and vice versa.

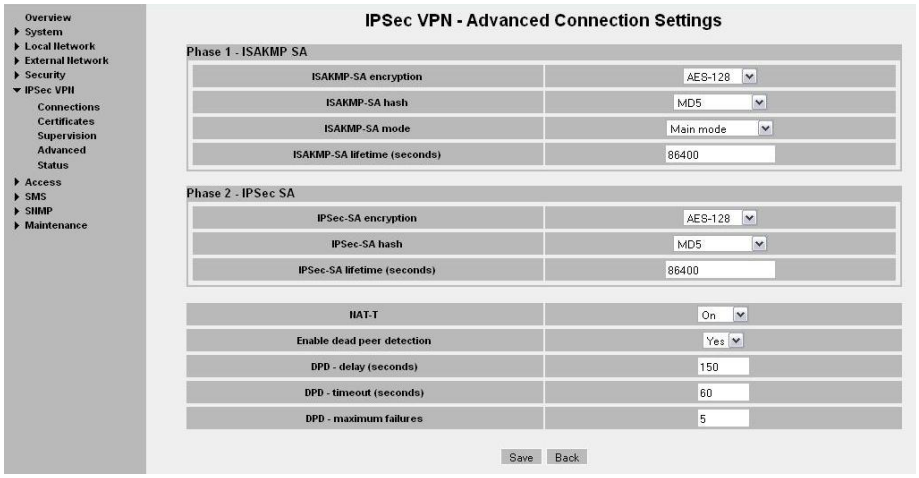
For authentication with X.509 certificate or CA certificate:

- If you keep the factory setting *NONE*, then the Distinguished Names from the own certificate and from the certificate communicated by the remote station are automatically used as the Local ID and Remote ID.
- If you manually change the entry for the Local ID or the Remote ID, then the corresponding entries must be adapted at the remote station. The manual entry for Local or Remote ID must be made in the ASN.1 format, e.g. "C=XY/O=XY Org/CN=xy.org.org"

For authentication with pre-shared secret key (PSK):

- In Roadwarrior Mode the Remote ID must be entered manually. The Remote ID must have the format of a hostname (e.g. RemoteStation.de) or the format of an e-mail address (remote@station.de), and must be the same as the Local ID of the remote station.
  The Local ID can be left on *NONE*. In this case the IP address is used as the local IP address. If you enter a Local ID; then it must have the format of a hostname (e.g. RemoteStation.de) or the format of an e-mail address (remote@station.de), and must be the same as the Local ID of the remote station.

Roadwarrior Mode
Edit IKE



Function

Here you can define the properties of the VPN connection according to your requirements and what you have agreed with the system administrator of the remote station.

ISAKMP-SA encryption

IPsec-SA encryption

Agree with the administrator of the remote station which encryption method will be used for the ISAKMP-SA and the IPsec-SA. The TAINY xMOD-V2-IO supports the following methods:

- 3DES-192
- AES-128
- AES-192
- AES-256

AES-128 is the most frequently used method, and is therefore set as the default.

The method can be defined differently for ISAKMP-SA and IPsec-SA.

Note:
The more bits in the encryption algorithm - indicated by the appended number - the more secure it is. The method AES-256 is therefore considered the most secure. However, the longer the key, the more time the encryption process takes and the more computing power is required.

ISAKMP-SA hash

IPsec-SA hash

Agree with the administrator of the remote station which method will be used for computing checksums/hashes during the ISAKMP phase and the IPsec phase. The following selections are available:

- MD5 or SHA-1 (automatic detection)
- MD5
- SHA-1

The method can be defined differently for ISAKMP-SA and IPsec-SA.

ISAKMP-SA mode

Agree with the administrator of the remote station which method will be used for negotiating the ISAKMP-SA. The following selections are available:

- Main mode
- Aggressive mode

Note:

When the authentication method Pre-Shared Key is used, Aggressive mode must be set in Roadwarrior mode.

ISAKMP-SA lifetime

IPsec-SA lifetime

The keys for an IPsec connection are renewed at certain intervals in order to increase the effort required to attack an IPsec connection.

Specify the lifetime (in seconds) of the keys agreed on for the ISAKMP-SA and IPsec-SA.

The lifetime can be defined differently for ISAKMP-SA and IPsec-SA.

NAT-T

There may be a NAT router between the TAINY xMOD-V2-IO and the VPN gateway of the remote network. Not all NAT routers allow IPsec data packets to go through. It may therefore be necessary to encapsulate the IPsec data packets in UDP packets so that they can go through the NAT router.

On: If the TAINY xMOD-V2-IO detects a NAT router that does not let the IPsec data packets through, then UDP encapsulation is started automatically.

Force: During negotiation of the connection parameters for the VPN connection, encapsulated transmission of the data packets during the connection is insisted upon.

Off: The NAT-T function is switched off

Enable dead peer detection

If the remote station supports the dead peer detection (DPD) protocol, then the partner in question can detect whether the IPsec connection is still valid or not, meaning that it may have to be re-established. Without DPD, depending on the configuration it may be necessary to wait until the SA lifetime elapses or the connection has to be re-initiated manually. To check whether the IPsec connection is still valid, the dead peer detection sends DPD requests to the remote station itself. If there is no answer, then after the permitted number of failed attempts the IPsec connection is considered to be interrupted.

Warning

Sending the DPD requests and using NAT-T increases the amount of data sent and received over the mobile data service connection (HSDPA, UMTS, EGPRS, GPRS). Depending on the selected settings, the additional data traffic can amount to 5 Mbyte per month or more. This can lead to additional costs.

Yes Dead peer detection is switched on. Independently of the transmission of user data, the TAINY xMOD-V2-IO detects if the connection is lost, in which case it waits for the connection to be re-established by the remote stations.

No Dead peer detection is switched off

DPD - delay (seconds)

Time period in seconds after which DPD requests will be sent. These requests test whether the remote station is still available.

DPD - timeout (seconds)

Time period in seconds after which the connection to the remote station will be declared dead if no response has been made to the DPD requests.

DPD – maximum failures — Number of failed attempts permitted before the IPsec connection is considered to be interrupted.

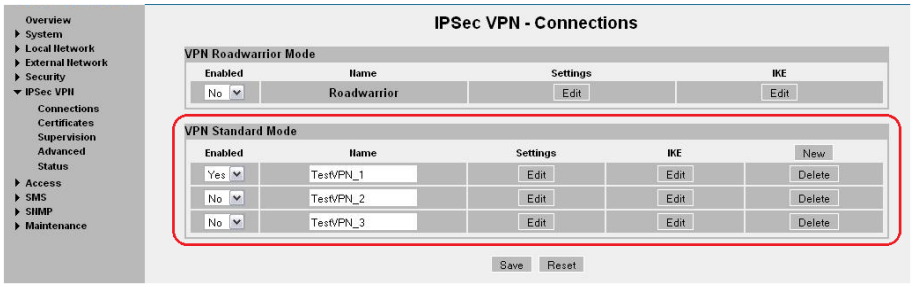
Factory setting — The factory settings for the TAINY xMOD-V2-IO are as follows:

Name	**Any**
Enabled	**No (switched off)**
Authentication method	**CA certificate**
Remote ID	**NONE**
Local ID	**NONE**
Remote certificate	**-**
ISAKMP-SA encryption	**AES-128**
IPsec-SA encryption	**AES-128**
ISAKMP-SA hash	**MD5**
IPsec-SA hash	**MD5**
ISAKMP-SA mode	**Main**
ISAKMP-SA lifetime (seconds)	**86400**
IPsec-SA lifetime (seconds)	**86400**
NAT-T	**On**
Enable dead peer detection	**Yes**
DPD - delay (seconds)	**150**
DPD – timeout (seconds)	**60**
DPD – maximum failures	**5**

7.3 VPN IPsec Standard Mode

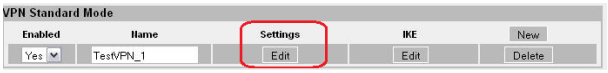
IPsec VPN > Connections

ONLY TAINY HMOD-V2-IO
ONLY TAINY EMOD-V2-IO

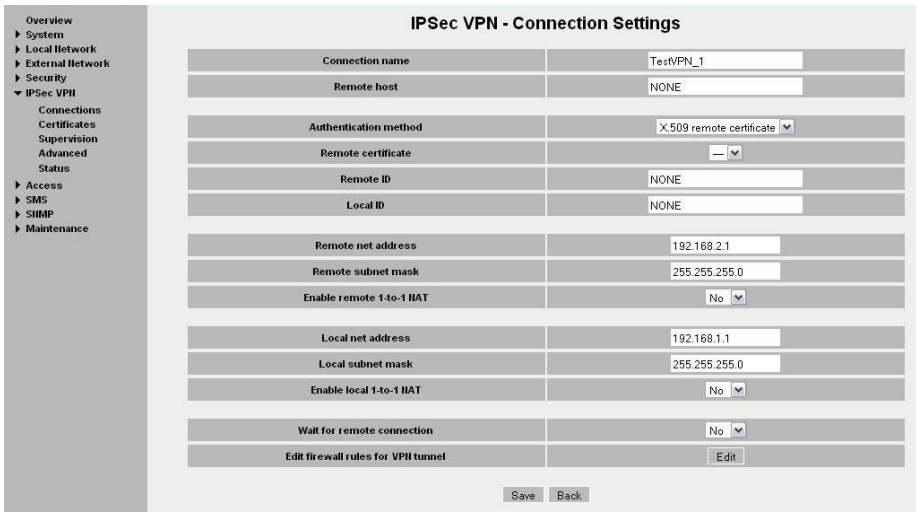


Function — The VPN connections already created are shown. You can enable (Enabled = *Yes*) or disable (Enabled = *No*) each individual connection. You can use *New* to add additional VPN connections, *Edit Settings* and *Advanced Settings* to set them up, and *Delete* to remove a connection.

VPN Standard Mode

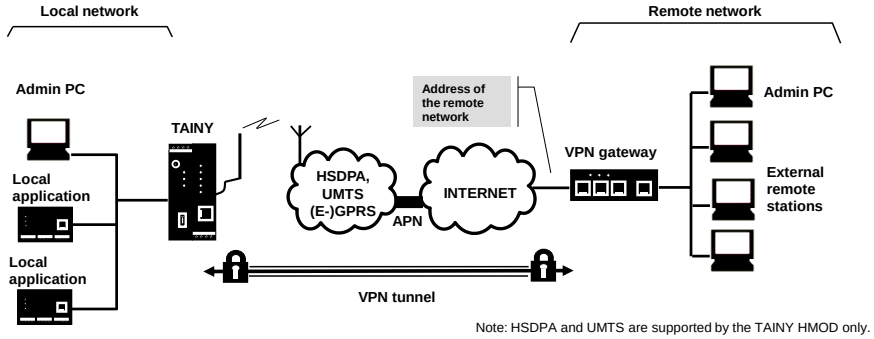


Edit Settings



Connection name — Give the new connection a connection name here.

Remote host — Specify the address of the remote station here, either as a hostname (e.g. myadress.com) or as an IP address.



Note: HSDPA and UMTS are supported by the TAINY HMOD only.

X.509 certificate, CA certificate

In the authentication methods X.509 certificate and CA certificate, the keys used for authentication have first been signed by a Certification Authority (CA). This method is considered especially secure. A CA can be a service provider, but also, for example, the system administrator for your project, provided that he has the necessary software tools. The CA creates a certificate file (PKCS12) with the file extension *p12 for each of the two remote stations. This certificate file contains the public and private keys for the own station, the signed certificate from the CA, and the public key of the CA. For the authentication method X.509 there is additionally a key file (*.pem or *.crt) for each of the two remote stations with the public key of the own station.

X.509 certificate — The public keys (files with extension *.pem or *.crt) are exchanged between the TAINY xMOD-V2-IO and the remote station's VPN gateway takes place manually, for example on a CD-ROM or via e-mail. To load the certificate, proceed as described in Chapter 7.4.

CA certificate — The public keys are exchanged between the TAINY xMOD-V2-IO and the remote station's VPN gateway via the data connection when the VPN connection is established. Manual exchange of the key files is not necessary.

Pre-shared secret key (PSK)

This method is primarily supported by older IPsec implementations. Here authentication is performed with a character string agreed on beforehand. In order to obtain high security, the character string should consist of about randomly-selected 30 lower-case and upper-case letters and numerals.

The following characters are permitted:

! $ % & ' ( ) * + , . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ ` a b c d e f g h I j k l m n o p q r s t u v w x y z { | } #

The entry is concealed.

Remote ID

Local ID

The Local ID and the Remote ID are used by IPsec to identify the remote stations uniquely when establishing the VPN connection.

For authentication with X.509 certificate or CA certificate:

- If you keep the factory setting *NONE*, then the Distinguished Names from the own certificate and from the certificate communicated by the remote station are automatically applied and used as the Local ID and Remote ID.
- If you manually change the entry for the Local ID or the Remote ID, then the corresponding entries must be adapted at the remote station. The own Local ID must be the same as the Remote ID of the remote station and vice versa. The entries for Local or Remote IDs must be made in the ASN.1 format, e.g. "C=XY/O=XY Org/CN=xy.org.org"

For authentication with pre-shared secret key (PSK):

- If you keep the factory setting *NONE*, then the own IP address is automatically used as the Local ID, and the IP address of the remote station is used as the Remote ID:
- If you manually change the entry for the Local ID or for the Remote ID, then the entries must have the format of a hostname (e.g. RemoteStation.de) or the format of an e-mail address (remote@station.de). The own Local ID must be the same as the Remote ID of the remote station and vice versa.

Note:

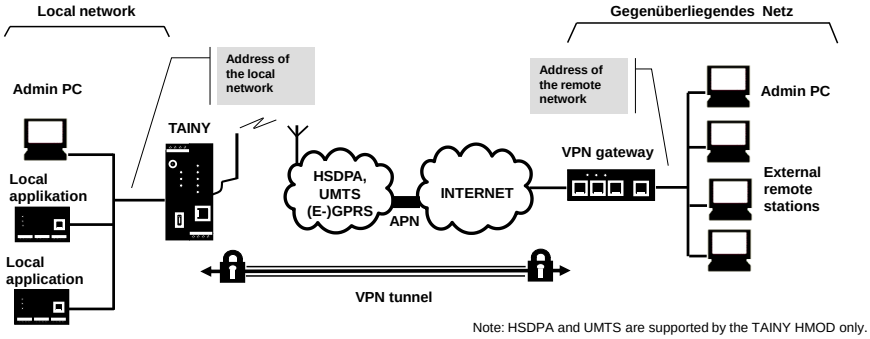
If with pre-shared secret key (PSK) the IP address is not used as the Remote ID, then the Aggressive Mode has to be set as the ISAKMP-SA mode.

Wait for remote connection

Yes	The TAINY xMOD-V2-IO waits for the VPN gateway of the remote network to initiate establishment of the VPN connection.
No	The TAINY xMOD-V2-IO initiates establishment of the connection.

Remote net address

Here enter the IP address (e.g. 123.123.123.123) of the remote network. The remote network can also be only a single computer.



Remote subnet mask

Here enter the subnet mask (e.g. 255.255.255.0) of the remote network. The remote network can also be only a single computer.

Activate 1-to-1 NAT for the remote network

The TAINY xMOD-V2-IO has a 1-to-1 NAT function for the remote network.

In TAINY xMOD-V2-IO, the address range of the remote network on the VPN connection is defined by the

- address of the remote network and the
- network mask of the remote network

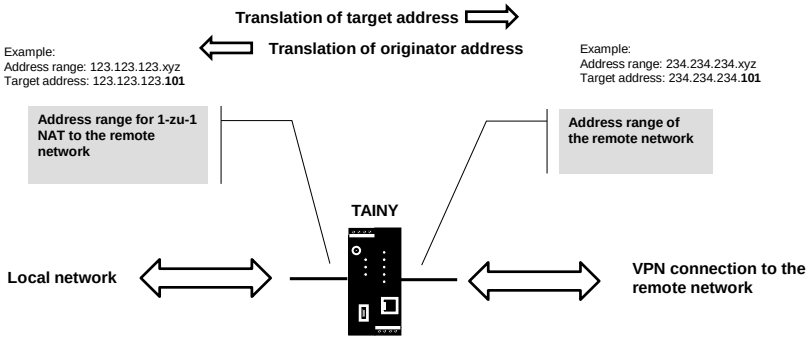
If 1-to-1 NAT is switched off, local applications must use this address range for the addressing of remote locations in the remote network.

A locally used address range through which the local applications can address the remote locations in the remote network can be defined when 1-to-1 NAT is activated.

The 1-to-1 NAT function in TAINY xMOD-V2-IO then maps the locally defined address range of the remote network on the address range of the remote network on the VPN connection.

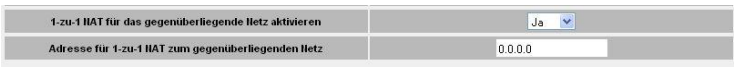
The locally used address range of the remote network is defined by the

- address for 1-to-1 NAT for the remote network and the
- network mask of the remote network



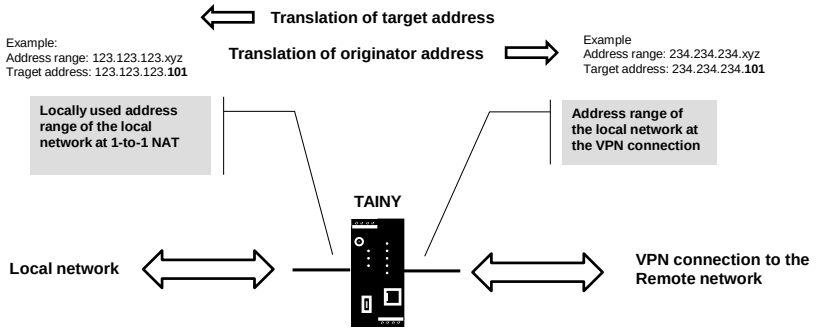
Yes

The TAINY xMOD-V2-IO uses 1-to-1 NAT for the remote network.

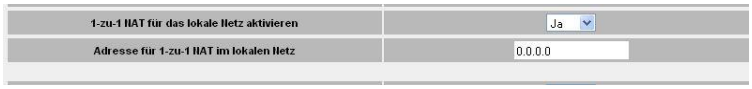


Enter the locally used target address as the address for 1-to-1 NAT for the remote network.

	No	The TAINY xMOD-V2-IO does not use 1-to-1 NAT for the remote network.
Local net address	Here enter the IP address (e.g. 123.123.123.123) of the local network. The local network can also be only a single computer.	
Local subnet mask	Here enter the subnet mask (e.g. 255.255.255.0) of the local network. The local network can also be only a single computer.	
Activate 1-to-1 NAT for the local network	In TAINY xMOD-V2-IO, the address range of the local network on the VPN connection is defined by the - address of the local network and the - network mask of the local network If 1-to-1 NAT is disabled, the addresses of local application must be within this address range, that they can be addressed via the VPN connection by the remote stations within the remote network. If 1-to-1 NAT is activated, a locally used address range fort he local network can be defined, which may differ from the address range used at the VPN connection. The 1-to-1 NAT function of the TAINY xMOD-V2-IO maps the local address range of the local network into the address range of the VPN connection. The locally used address range of the local network is defined by the - address of the 1-to-1-NAT within the local network and the - network mask of the local network	


Translation of target address
Example:
Address range: 123.123.123.xyz
Traget address: 123.123.123.101
Translation of originator address
Example
Address range: 234.234.234.xyz
Target address: 234.234.234.101
Locally used address range of the local network at 1-to-1 NAT
Address range of the local network at the VPN connection
TAINY
Local network
VPN connection to the Remote network

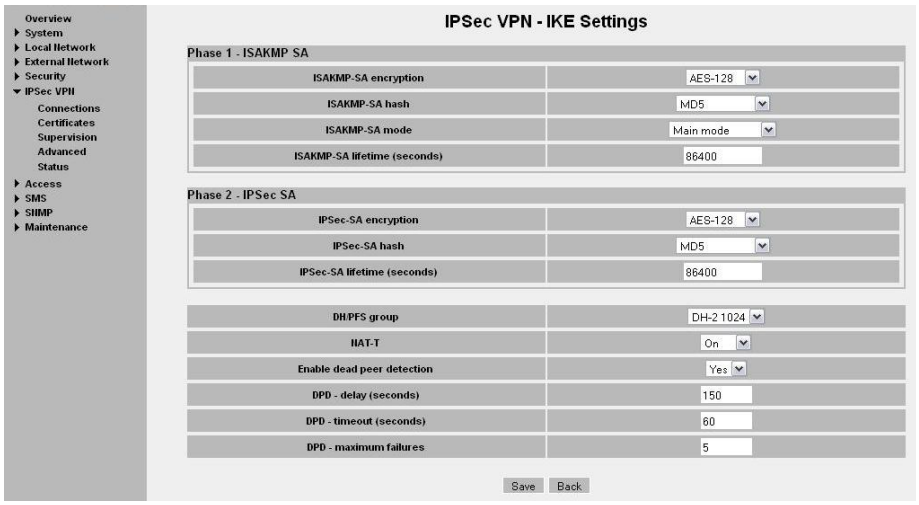
	Yes	The TAINY xMOD-V2-IO uses 1-to-1-NAT to the local network..



		Enter as the address for 1-zu-1-NAT in the local nework the locally used target address.
	No	The TAINY xMOD-V2-IO uses no 1-to-1-NAT to the local network.
Firewall rules for VPN tunnel	See Chapter 0	

VPN Standard Mode

Edit IKE



Function

Here you can define the properties of the VPN connection according to your requirements and what you have agreed with the system administrator of the remote station.

ISAKMP-SA encryption

IPsec-SA encryption

Agree with the administrator of the remote station which encryption method will be used for the ISAKMP-SA and the IPsec-SA. The TAINY xMOD-V2-IO supports the following methods:

- 3DES-192
- AES-128
- AES-192
- AES-256

AES-128 is the most frequently used method, and is therefore set as the default.

The method can be defined differently for ISAKMP-SA and IPsec-SA.

Note:
The more bits in the encryption algorithm - indicated by the appended number - the more secure it is. The method AES-256 is therefore considered the most secure. However, the longer the key, the more time the encryption process takes and the more computing power is required.

ISAKMP-SA hash

IPsec-SA hash

Agree with the administrator of the remote station which method will be used for computing checksums/hashes during the ISAKMP phase and the IPsec phase. The following selections are available:

- MD5 or SHA-1 (automatic detection)
- MD5
- SHA-1

The method can be defined differently for ISAKMP-SA and IPsec-SA.

ISAKMP-SA mode

Agree with the administrator of the remote station which method will be used for negotiating the ISAKMP-SA. The following selections are available:

- Main mode
- Aggressive mode

DH/PFS group
Agree with the administrator of the remote station the DH group for the key exchange.

ISAKMP-SA lifetime
IPsec-SA lifetime
The keys for an IPsec connection are renewed at certain intervals in order to increase the effort required to attack an IPsec connection.

Specify the lifetime (in seconds) of the keys agreed on for the ISAKMP-SA and IPsec-SA.

The lifetime can be defined differently for ISAKMP-SA and IPsec-SA.

NAT-T
There may be a NAT router between the TAINY xMOD-V2-IO and the VPN gateway of the remote network. Not all NAT routers allow IPsec data packets to go through. It may therefore be necessary to encapsulate the IPsec data packets in UDP packets so that they can go through the NAT router.

On: If the TAINY xMOD-V2-IO detects a NAT router that does not let the IPsec data packets through, then UDP encapsulation is started automatically.

Force: During negotiation of the connection parameters for the VPN connection, encapsulated transmission of the data packets during the connection is insisted upon.

Off: The NAT-T function is switched off

Enable dead peer detection
If the remote station supports the dead peer detection (DPD) protocol, then the partner in question can detect whether the IPsec connection is still valid or not, meaning that it may have to be re-established. Without DPD, depending on the configuration it may be necessary to wait until the SA lifetime elapses or the connection has to be re-initiated manually. To check whether the IPsec connection is still valid, the dead peer detection sends DPD requests to the remote station itself. If there is no answer, then after the permitted number of failed attempts the IPsec connection is considered to be interrupted.

Warning

Sending the DPD requests and using NAT-T increases the amount of data sent and received over the mobile data service connection (HSDPA, UMTS, EGPRS, GPRS). Depending on the selected settings, the additional data traffic can amount to 5 Mbyte per month or more. This can lead to additional costs.

Yes Dead peer detection is switched on. Attempts are made to re-establish the IPsec connection if it has been declared dead, independently of the transmission of user data.

No Dead peer detection is switched off

DPD - delay (seconds)
Time period in seconds after which DPD requests will be sent. These requests test whether the remote station is still available.

DPD - timeout (seconds)
Time period in seconds after which the connection to the remote station will be declared dead if no response has been made to the DPD requests.

DPD – maximum failures
Number of failed attempts permitted before the IPsec connection is considered to be interrupted.

Factory setting

The factory settings used by the TAINY xMOD-V2-IO for a newly created connection are as follows:

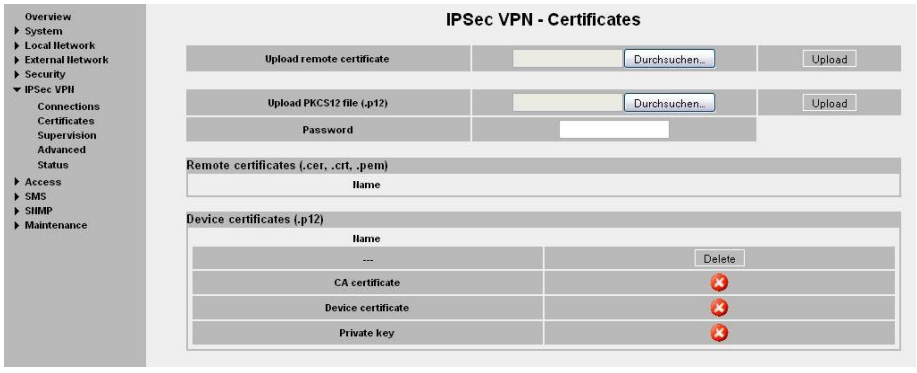
Name	**NewConnection**
Enabled	**No (switched off)**
Authentication method	**CA certificate**

Remote ID	**NONE**
Local ID	**NONE**
Remote certificate	**-**
Wait for remote connection	**No**
Remote net address	**192.168.2.1**
Remote subnet mask	**255.255.255.0**
Local net address	**192.168.1.1**
Local subnet subnet mask	**255.255.255.0**
ISAKMP-SA encryption	**AES-128**
IPsec-SA encryption	**AES-128**
ISAKMP-SA hash	**MD5**
IPsec-SA hash	**MD5**
DH/PFS group	**DH-2 1024**
ISAKMP-SA mode	**Main**
ISAKMP-SA lifetime (seconds)	**86400**
IPsec-SA lifetime (seconds)	**86400**
NAT-T	**On**
Enable dead peer detection	**Yes**
DPD - delay (seconds)	**150**
DPD – timeout (seconds)	**60**
DPD – maximum failures	**5**

7.4 Loading VPN certificates

IPsec VPN > Connections

ONLY TAINY HMOD-V2-IO
ONLY TAINY EMOD-V2-IO



Function	Loading and administering certificates and keys.
Upload remote certificate	Here load key files (*.pem, *.crt) with remote certificates and public key from remote stations into the TAINY xMOD-V2-IO. To do this, the files must be saved on the Admin PC. A remote certificate is only required for the authentication method with X.509 certificate.

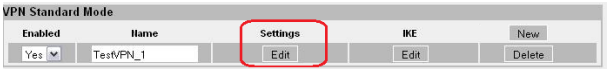
Upload PKCS12 file (.p12)	Here load the certificate file (PKCS12 file) with the file extension .p12 into the TAINY xMOD-V2-IO. To do this, the certificate file must be saved on the Admin PC.
	Caution If there is already a certificate file in the device, then it must be deleted before loading a new file.
Password	The certificate file (PKCS12 file) is password-protected. Here enter the password that you received with the certificate file.
Remote certificates (.crt)	A list with all of the loaded remote certificates is shown here. You can use *Delete* to remove a remote certificates that is no longer needed.
Device certificates (.p12)	The name and status of the loaded certificate file (PKCS12 file) is shown here. The corresponding component of the certificate file is present The corresponding component is missing or that the wrong password was entered.

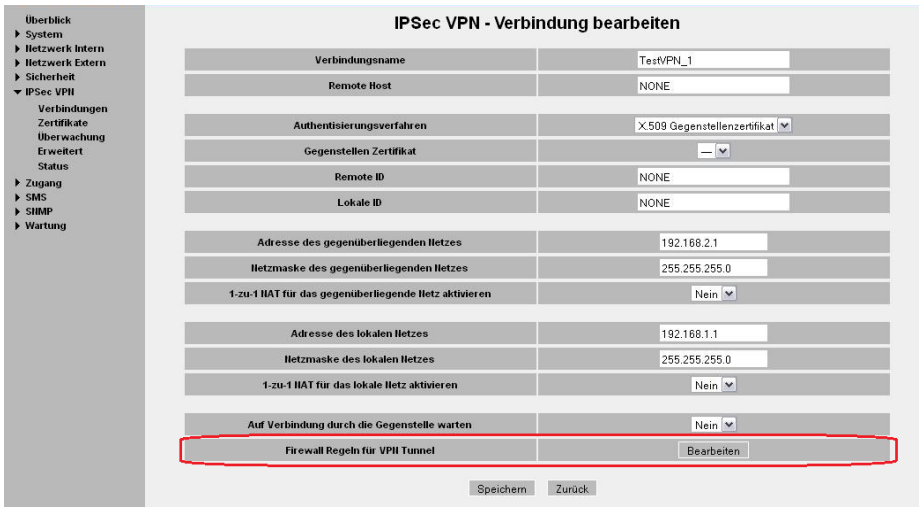
7.5 Firewall rules for VPN tunnel

Firewall rules for VPN tunnel

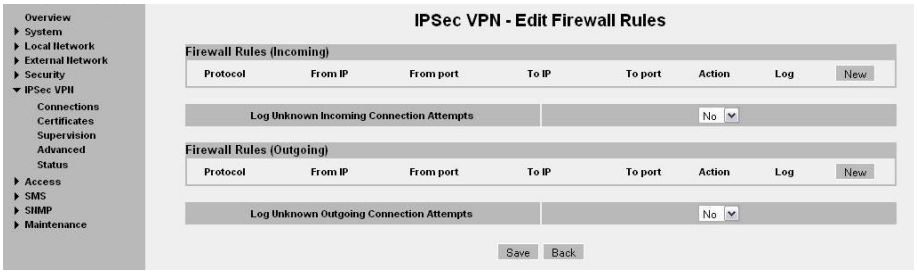
ONLY TAINY HMOD-V2-IO
ONLY TAINY EMOD-V2-IO

The user interface for setting up the firewall rules for VPN tunnels can be found under IPsec VPN > Connections:





IPsec VPN – Edit Firewall Rules



Function

The IPsec VPN connection is viewed as fundamentally secure. Thus data traffic over this connection is not limited by default. It is possible, however, to create firewall rules for the VPN connection

To set up firewall rules for the VPN connection, proceed in the same way as for setting up the packet filter function of the general firewall (see Chapter 6.1). However, the rules defined here apply only to the specific VPN connection.

Factory setting

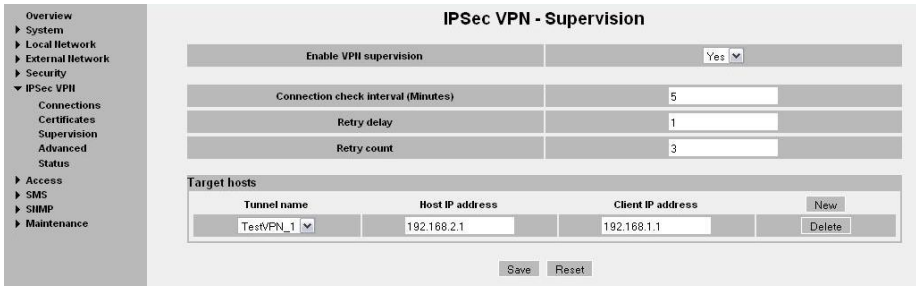
The factory settings used by the TAINY xMOD-V2-IO for a newly created connection are as follows:

Firewall rules for VPN tunnel **No limitations**

7.6 Supervision of VPN connections

IPsec VPN – Supervision

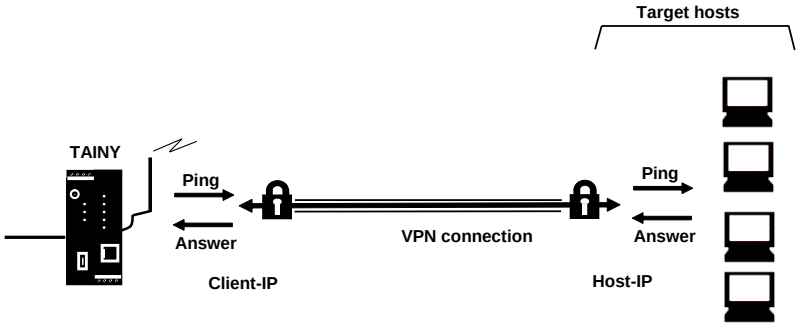
ONLY TAINY HMOD-V2-IO
ONLY TAINY EMOD-V2-IO



Function

With the supervision of VPN connections the TAINY xMOD-V2-IO checks the condition of configured VPN connections. To check the VPN connection status the TAINY xMOD-V2-IO sends periodically ping packets (ICMP) via the VPN connection to one or several remote stations (target hosts). This is made independently from payload data. For each VPN connection an own supervision can be configured.

If the TAINY xMOD-V2-IO receives the answer for the ping packet from at least one addressed remote station, the VPN connection is still operational.



If no remote station answers the ping packet the transmission of the ping packet will be repeated several times after a delay which can be configured. If all repetitions end without success, the VPN client in the TAINY HMOD-V2-IO will be restarted. This causes a reconnection of all existing VPN connections.

Warning

Sending the ping packages (ICMP) increases the amount of data sent and received over the mobile data service connection (HSDPA, UMTS, EGPRS or GPRS). Depending on the selected settings, the additional data traffic can amount to 4.5 Mbyte per month or more. This can lead to additional costs.

Note

The supervision of the VPN connections by ping partly overlaps the monitoring functions of Dead Peer Detection. Ping supervision activated can increase the DPD delay.

Enable VPN supervision	*Yes*	VPN supervision on
	No	VPN supervision off
Connection check interval	This parameter determines the time interval to send ping packets through the supervised VPN connection (VPN tunnel). The value shall be given in minutes.	
Retry delay	This parameter determines the delay a ping packet is repeated after a failed ping check (ping packet not answered). The value shall be given in minutes.	
Retry count	This parameter determines the number of allowed failed ping transmission retries before the VPN client inside the TAINY HMOD-V2-IO will be restarted.	
Target hosts	*Tunnel name*	Determine, which VPN connection (VPN tunnel) shall be supervised. Add a VPN connection by clicking the *New* button, delete a VPN connection by clicking the *Delete* button.
	Host IP address	Enter the IP address of the remote station (target host) here.
	Client IP address	Enter here any unused IP address of the local network related to the VPN connection.

Factory setting

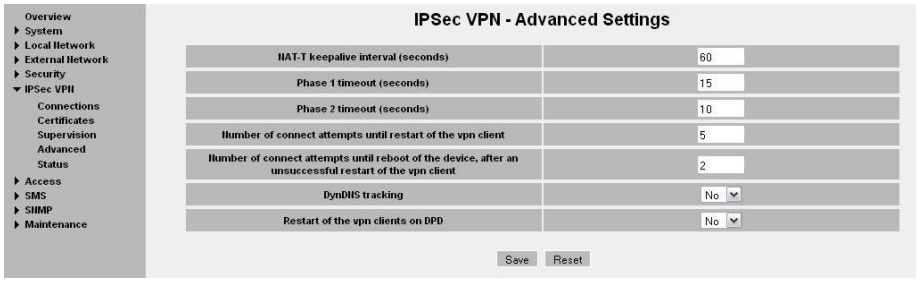
The factory settings used by the TAINY xMOD-V2-IO are as follows:

Enable VPN supervision	**Nein**
Connection check interval (minutes)	**5**
Retry delay (minutes)	**1**
Retry count	**3**

7.7 Advanced settings for VPN connections

IPsec VPN > Advanced settings

ONLY TAINY HMOD-V2-IO
ONLY TAINY EMOD-V2-IO



Function	Setting special timeouts and intervals for VPN connections.
NAT-T keepalive interval (seconds)	If NAT-T is enabled (cf. Chapter 7.3), then keepalive data packets will be sent periodically by the TAINY xMOD-V2-IO through the VPN connection. The purpose of this is to prevent a NAT router between the TAINY xMOD-V2-IO and the remote station from interrupting the connection during idle periods without data traffic. Here you can change the interval between the keepalive data packets.
Phase 1 timeout (seconds)	The Phase 1 timeout determines how long the TAINY xMOD-V2-IO waits for completion of an authentication process of the ISAKMP-SA. If the set timeout is exceeded, the authentication will be aborted and restarted. Here you change the timeout.
Phase 2 timeout (seconds)	The Phase 2 timeout determines how long the TAINY xMOD-V2-IO waits for completion of an authentication process of the IPsec-SA. If the set timeout is exceeded, the authentication will be aborted and restarted. Here you change the timeout.
Number of connects attempts until restart of the VPN client	If the establishment of a VPN connection fails, the connection setup will be retried by the TAINY xMOD-V2-IO. Enter the number of unsuccessful retries, being performed before the TAINY xMOD-V2-IO restart its VPN client before trying again the connection setup.
Number of connect attempts until reboot of the device, after an unsuccessful restart of the VPN client	If the establishment of a VPN connection fails, the connection setup will be retried by the TAINY xMOD-V2-IO. Enter the number of unsuccessful retries, being performed before the TAINY xMOD-V2-IO reboots and tries again the connection setup.
DynDNS Tracking	If the VPN gateway of the remote stations uses a DynDNS service to get an IP address and no Dead Peer Detection is used, the TAINY xMOD-V2-IO should periodically check, if the remote VPN gateway is still reachable. The DynDNS tracking function provides this function. *Yes* activates this function, *No* deactivate this function.
DynDNS Tracking Interval (Minutes)	Configure here the interval it shall be checked, if the remote station is still reachable.

Factory setting

The factory settings used by the TAINY xMOD-V2-IO are as follows:

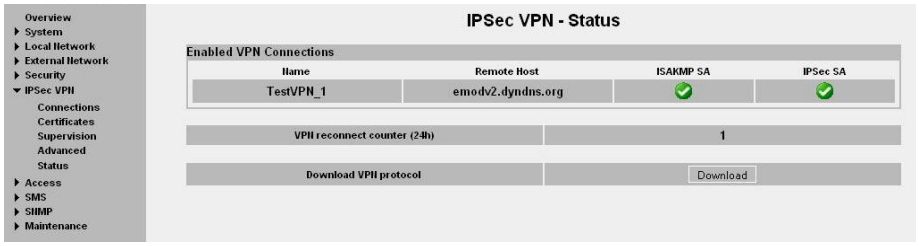
NAT-T keepalive interval (seconds)	**60**
Phase 1 timeout (seconds)	**15**
Phase 2 timeout (seconds)	**10**
Number of connects attempts until restart of the VPN client	**5**
Number of connect attempts until reboot of the device, after an unsuccessful restart of the VPN client	**2**

DynDNS Tracking	**No (Nein)**
DynDNS Tracking Interval (Minutes)	**5**
Restart of the VPN clients on DPD	**Nein**

7.8 Status of the VPN connections

IPsec VPN > Connections

ONLY TAINY HMOD-V2-IO
ONLY TAINY EMOD-V2-IO

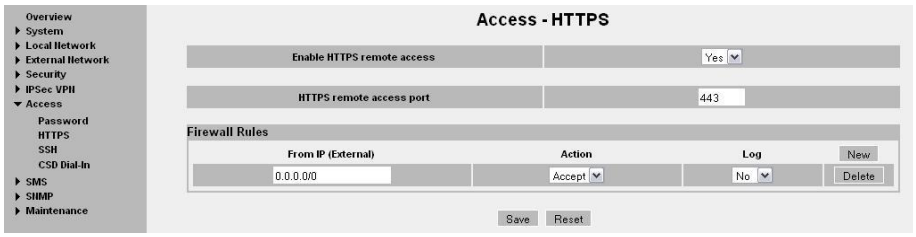


Function	Indicates the status of the enabled VPN connections and the option for loading a protocol file to the Admin PC.
Activated VPN connections	The respective security association (SA) has been successfully established. The security association has not been established.
VPN reconnect counter (24h)	Shows the number of attempts to establish the activated VPN connections since 0:00 (system time)
Download VPN protocol	This function can be used to download the VPN protocol file to the Admin PC.

8 Remote access

8.1 HTTPS remote access

Access > HTTPS



Function

The HTTPS remote access (= *HyperText Transfer Protocol Secure*) allows secure access to the Web user interface of the TAINY HMOD-V2-IO from an external network via HSDPA, UMTS, EGPRS, GPRS or CSD.

Configuration of the TAINY xMOD via the HTTPS remote access then takes place exactly like configuration via a Web browser via the local interface.

Enable HTTPS remote access

Yes — Access to the Web user interface of the TAINY xMOD from the external network via HTTPS is allowed.

No — Access via HTTPS is not allowed.

HTTPS remote access port

Default: 443 (factory setting)

Here you can define an alternative port. However, if you like to use the alternative port, the external remote station conducting the remote access must specify the port number after the IP address when specifying the address.

Example:
If this TAINY xMOD can be accessed via the Internet using the address 192.144.112.5, and if port number 442 has been defined for the remote access, then the following must be specified in the Web browser at the external remote station:
https://192.144.112.5:442

Note

Additionally to the new selected port, the standard port 443 for https remote access keeps open.

Firewall rules for HTTPS remote access

New — Adds a new firewall rule for HTTPS remote access that you can then fill out.

Delete — Removes a firewall rule for HTTPS remote access that has been created.

From IP (External) — Specify here the address(es) of the computer(s) for which remote access is allowed. You have the following options:

IP address or address range: **0.0.0.0/0** means all addresses. To specify a range, use the CIDR notation - see Chapter 11.

Action Define how access to the specified HTTPS port will be handled:

Accept means that the data packets can go through.

Reject means that the data packets are rejected, and the sender receives a message about the rejection.

Drop means that the data packets are not allowed through. They are discarded without the sender receiving any information about where they went.

Log For each individual firewall rule you can define whether the event should be logged when the rule takes effect - set *Log* to *Yes*,
or not - set *Log* to *No* (factory setting).

The log is kept in the firewall log, see Chapter 6.4.

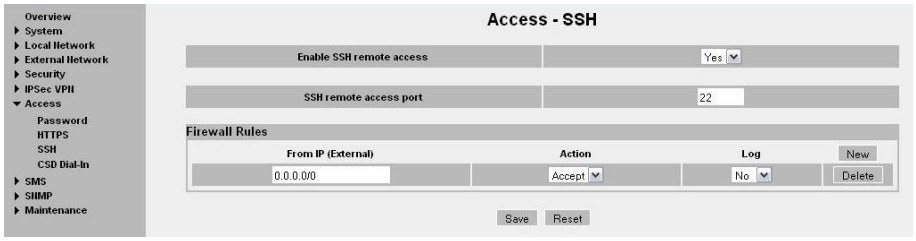
Factory setting

The factory settings for the TAINY xMOD are as follows:

Enable HTTPS remote access	**No (switched off)**
HTTPS remote access port	**443**
Default for new rules:	
From IP (External)	**0.0.0.0/0**
Action	**Accept**
Log	**No (switched off)**

8.2 Remote access – SSH

Access > SSH



Function

The SSH remote access (= *Secured SHell*) allows secure access to the file system of the TAINY xMOD from an external network via HSDPA, UMTS, EGPRS, GPRS or CSD.

To do this, a connection must be established using an SSH-capable program from the external remote station to the TAINY xMOD.

Use the SSH remote access only if you are familiar with the LINUX file system.

In the factory setting this option is deactivated.

Warning

Via SSH remote access it is possible to derange the configuration of the device in such a way that it will have to be sent in for servicing. In this case please contact your dealer or distributor.

Enable SSH remote access

Yes Access to the file system of the TAINY xMOD from the external network via SSH is allowed.

No Access via SSH is not allowed.

SSH remote access port

Default: 22 (factory setting)

You can define an alterative port. However, if you have defined an alternative port, then the external remote station conducting the remote access must specify the port number defined here in front of the IP address when specifying the address.

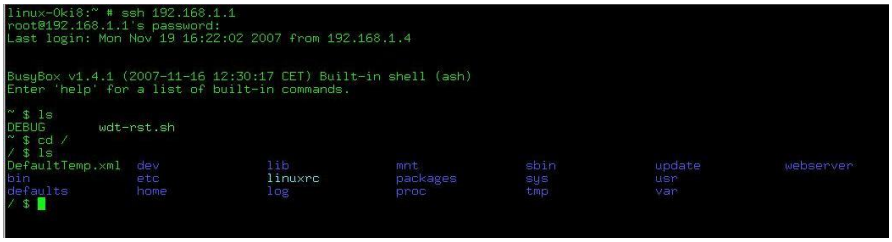
Note

Additionally to the new selected port, the standard port 22 for SSH remote access keeps open.

Example:
If this TAINY xMOD can be accessed from the external network using the address 192.144.112.5, and if port 22222 has been defined for the remote access, then this port number must be specified in the SSH client (e.g. PUTTY) at the external remote station:

SSH -p 22222 192.144.112.5

Example for console:


linux-Oki8:~ # ssh 192.168.1.1
root@192.168.1.1's password:
Last login: Mon Nov 19 16:22:02 2007 from 192.168.1.4
BusyBox v1.4.1 (2007-11-16 12:30:17 CET) Built-in shell (ash)
Enter 'help' for a list of built-in commands.
~ $ ls
DEBUG wdt-rst.sh
~ $ cd /
/ $ ls
DefaultTemp.xml dev lib mnt sbin update webserver
bin etc linuxrc packages sys usr
defaults home log proc tmp var
/ $

Firewall rules for SSH remote access

New — Adds a new firewall rule for SSH remote access that you can then fill out.

Delete — Removes a firewall rule for SSH remote access that has been created.

From IP (External) — Specify here the address(es) of the computer(s) for which remote access is allowed. You have the following options:

IP address or address range: **0.0.0.0/0** means all addresses. To specify a range, use the CIDR notation - see Chapter 11.

Action — Define how access to the specified SSH port will be handled:

Accept means that the data packets can go through.

Reject means that the data packets are rejected, and the sender receives a message about the rejection.

Drop means that the data packets are not allowed through. They are discarded without the sender receiving any information about where they went.

Log — For each individual firewall rule you can define whether the event should be logged when the rule takes effect - set *Log* to *Yes*,
or not - set *Log* to *No* (factory setting).

The log is kept in the firewall log, see Chapter 6.4.

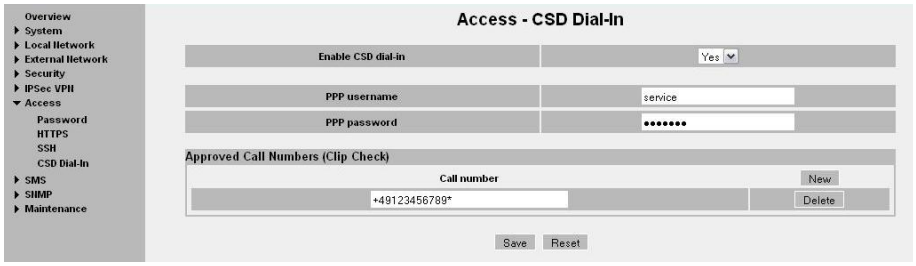
Factory setting

The factory settings for the TAINY xMOD are as follows:

Enable SSH remote access	**No (switched off)**
SSH remote access port	**22**
Default for new rules:	
From IP (External)	**0.0.0.0/0**
Action	**Accept**
Log	**No (switched off)**

8.3 Remote access via dial-in connection

Access > CSD Dial-In



Function

The CSD dial-in access makes it possible to access the Web user interface of the TAINY xMOD via a dial-in data connection (*CSD = Circuit Switched Data*). To do this, call the TAINY xMOD at the data call number using an analogue modem, or at the voice or data call number of its SIM card using a GSM modem. The TAINY xMOD accepts the call if:

- the call number of the telephone connection that you call from is saved in the list of permitted numbers in TAINY xMOD, and
- the call number is transmitted by the telephone network (CLIP function)

Dialling must be performed by a PPP client, for example via a Windows dial-up connection. In Windows, use the *New Connection Wizard*, and under *Connect to the network at my workplace* set up a *Dial-up connection*.

Web interface and ssh console have the IP address 10.99.99.1. in case of CSD Dial-In.

ONLY for TAINY HMOD

Note

This function is available only, if a GSM network is used. In UMTS networks, this function cannot be used.

Enable CSD dial-in

Yes	Access to the Web user interface of the TAINY xMOD from a dial-in data connection is allowed.
No	Access via dial-in data connection is not allowed.

PPP username / password

Select a username and a password that must be used by a PPP client (e.g. a Windows dial-up connection) to log on to the TAINY xMOD. The same username and the same password must be entered in the PPP client.

Approved Call Numbers

Specify the call number of the telephone connection from which the dial-in data connection is established. The telephone connection must support Calling Line Identification Presentation (CLIP), and this function must be activated.

The call number entered in the TAINY xMOD must be exactly the same as the call number reported, any may also have to include the country code and prefix, e.g. +494012345678.

If multiple call numbers of a private branch exchange are to have access authorisation, you can use the "*" symbol as a wildcard, e.g. +49401234*. Then all call numbers that begin with +49401234 will be accepted.

Note

Firewall rules entered for HTTPS and SSH access also apply for CSD access. The source IP address (*"From IP"*) for CSD access is defined as 10.99.99.2.

New Adds a new approved call number for CSD remote access that you can then fill out.

Delete Removes a firewall rule for CSD remote access.

Factory setting

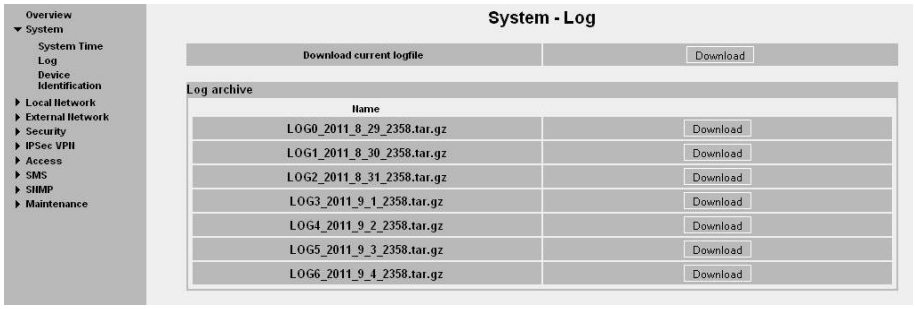
The factory settings for the TAINY xMOD are as follows:

Enable CSD dial-in	**No (switched off)**
PPP username	**service**
PPP password	**service**
Approved Call Numbers	*****

9 Status, log and diagnosis

9.1 Log

System > Log



Log

Important events in the operation of the TAINY xMOD are saved in the log.

- Reboot
- Changes to the configuration
- Establishing of connections
- Interruption of connections
- Signal strength
- etc.

The log is saved to the log archive of the TAINY xMOD when a file size 1 Mbyte, is reached, but after 24 hours at the latest.

Download current logfile

Download - the current log is loaded to the Admin PC. You can select the directory to save the file to, and can view the file there.

Log archive

Download - The archived log files are loaded to the Admin PC. You can select the directory to save the files to, and can view the files there.

Example:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
13.12.2007 11:04	3173XX	(null)	(null)	(null)	SERVICE_MASK=0	4	UH	41	CURRENT SYSTEM VERSION	1.014					
13.12.2007 19:46	3173XX	(null)	(null)	(null)	SERVICE_MASK=0	4	UH	41	CURRENT SYSTEM VERSION	1.014					
13.12.2007 19:46	3173XX	CSQ=---	STAT=---	COPS=---	SERVICE_MASK=495591	4	APL	0	SYSTEM STARTING	Success					
13.12.2007 19:47	3173XX	CSQ=---	STAT=---	COPS=---	(null)	0	APL	5	CONNECTION ERROR	Missing or incorrect GSM parameter					
13.12.2007 20:03	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:	RXS:	TX:0	RX:0;
13.12.2007 20:19	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:	RXS:	TX:0	RX:0;
13.12.2007 20:36	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:	RXS:	TX:0	RX:0;
13.12.2007 20:52	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:	RXS:	TX:0	RX:0;
13.12.2007 21:09	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:	RXS:	TX:0	RX:0;
13.12.2007 21:25	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:	RXS:	TX:0	RX:0;
14.12.2007 12:15	3173XX	(null)	(null)	(null)	SERVICE_MASK=0	4	UH	41	CURRENT SYSTEM VERSION	1.014					
14.12.2007 12:16	3173XX	CSQ=---	STAT=---	COPS=---	SERVICE_MASK=495591	4	APL	0	SYSTEM STARTING	Success					
14.12.2007 12:16	3173XX	CSQ=---	STAT=---	COPS=---	SERVICE_MASK=495591	0	APL	5	CONNECTION ERROR	Missing or incorrect GSM parameter					
14.12.2007 12:16	3173XX	CSQ=---	STAT=---	COPS=---	SERVICE_MASK=495591	4	CH	9	CONFIGURATION FILE ACCESS	(write values)					
14.12.2007 12:16	3173XX	CSQ=---	STAT=---	COPS=---	SERVICE_MASK=495591	4	CH	9	CONFIGURATION FILE ACCESS	InternalIPs.InternalIP_0.IP:192.168.1.1					
14.12.2007 12:16	3173XX	CSQ=---	STAT=---	COPS=---	SERVICE_MASK=495591	4	CH	9	CONFIGURATION FILE ACCESS	InternalIPs.InternalIP_0.NetMask:255.255.255.0					
14.12.2007 12:16	3173XX	CSQ=---	STAT=---	COPS=---	(null)	4	CH	9	CONFIGURATION FILE ACCESS	InternalIPs.InternalIP_1.IP:192.168.0.20					
14.12.2007 12:16	3173XX	CSQ=---	STAT=---	COPS=---	(null)	4	CH	9	CONFIGURATION FILE ACCESS	InternalIPs.InternalIP_1.NetMask:255.255.255.0					
14.12.2007 23:05	3173XX	(null)	(null)	(null)	SERVICE_MASK=0	4	UH	41	CURRENT SYSTEM VERSION	1.014					
14.12.2007 23:05	3173XX	CSQ=---	STAT=---	COPS=---	SERVICE_MASK=495591	4	APL	0	SYSTEM STARTING	Success					
14.12.2007 23:05	3173XX	CSQ=---	STAT=---	COPS=---	(null)	0	APL	5	CONNECTION ERROR	Missing or incorrect GSM parameter					
14.12.2007 23:08	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	CH	9	CONFIGURATION FILE ACCESS	(write values)					
14.12.2007 23:09	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	CH	9	CONFIGURATION FILE ACCESS	(write values)					
14.12.2007 23:09	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	3	GPRS CONNECTION ESTABLISHED	GPRS connect					
14.12.2007 23:10	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	8	IP ASSIGNED	172.25.105.9					
14.12.2007 23:11	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	CH	9	CONFIGURATION FILE ACCESS	(write values)					
14.12.2007 23:11	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	CH	9	CONFIGURATION FILE ACCESS	ICMPCheck.Enabled:true					
14.12.2007 23:11	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495615	4	CH	9	CONFIGURATION FILE ACCESS	(write values)					
14.12.2007 23:11	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495615	4	CH	9	CONFIGURATION FILE ACCESS	ICMPCheck.Enabled:true					
14.12.2007 23:12	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495615	4	CH	9	CONFIGURATION FILE ACCESS	(write values)					
14.12.2007 23:12	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495615	4	CH	9	CONFIGURATION FILE ACCESS	ICMPCheck.Enabled:true					
14.12.2007 23:13	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495615	4	CH	9	CONFIGURATION FILE ACCESS	(write values)					
14.12.2007 23:13	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495615	4	CH	9	CONFIGURATION FILE ACCESS	NTP.Enabled:true					
14.12.2007 22:24	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=499711	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:449	RXS:358	TX:1078	RX:358;
14.12.2007 22:40	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=499711	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:449	RXS:358	TX:1078	RX:358;
14.12.2007 22:57	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=499711	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:449	RXS:358	TX:1078	RX:358;
14.12.2007 23:13	3173XX	CSQ=10	STAT=1	COPS=26201	SERVICE_MASK=499711	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:449	RXS:358	TX:1078	RX:358;
14.12.2007 23:30	3173XX	CSQ=10	STAT=1	COPS=26201	SERVICE_MASK=499711	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:2737	RXS:3931	TX:3366	RX:3931;
14.12.2007 23:46	3173XX	CSQ=10	STAT=1	COPS=26201	SERVICE_MASK=499711	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:3089	RXS:4469	TX:3718	RX:4469;

Entries in log

Column A: Time stamp

Column B: Dr. Neuhaus product number

Column C: Signal quality (CSQ value)

Column D: GSM login status

STAT = --- = Function not activated yet

STAT = 1 = Logged in to home network

STAT = 2 = Not logged in; searching for network

STAT = 3 = Login rejected

STAT = 5 = Logged in to third-party network (roaming)

Column E: Indication of the network operator identification with the 3-digit country code (MCC) and the 2-3-digit network operator code (MNC).

Example: 26201 (262 = country code / 01 = network operator code)

Column F: Coded operating status (for customer service)

Column G: Category of the log report (for customer service)

Column H: Internal source of the log report (for customer service)

Column I: Internal report number (for customer service)

Column J: Log report in plain text

Columns K-P: Additional information on the plain text report, such as:

- Cell ID (identification number of the active GSM cell)

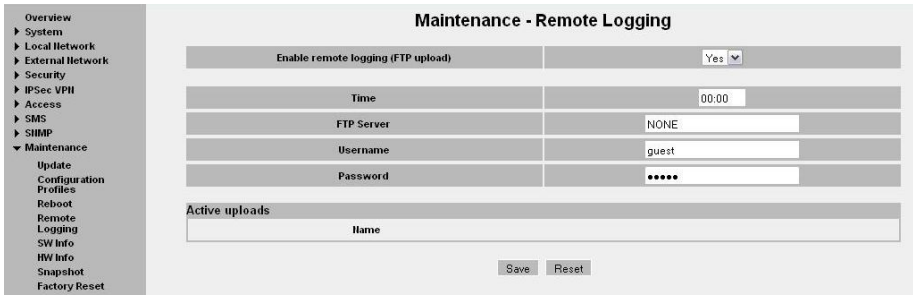
- Software version

- TXS, RXS (IP packets transmitted in the current connection)

- TX, RX (IP packets transmitted since the last factory settings reboot)

9.2 Remote logging

Maintenance > Remote Logging



Function

The TAINY xMOD can transfer the system log once per day via FTP (= File Transfer Protocol) to an FTP server.

The current system log and the system log files in the archive are transferred. After successful transfer the transferred logs are deleted in the TAINY xMOD.

If the transfer fails, the TAINY xMOD -IO tries once again to transfer the data after 24 hours.

Note

After an unsuccessful FTP upload, the log files are stored under Maintenance > Remote Logging.

Enable remote logging (FTP upload)

Yes activates the function.

Time

Specifies the *Time* at which the logs are to be transferred.

FTP Server

Specifies the address of the *FTP server* to which the log files are to be transferred. The address can be specified as a hostname (e.g. ftp.server.de) or as an IP address.

Username

Specifies the username for logging in to the FTP server.

Password

Specifies the password for logging in to the FTP server.

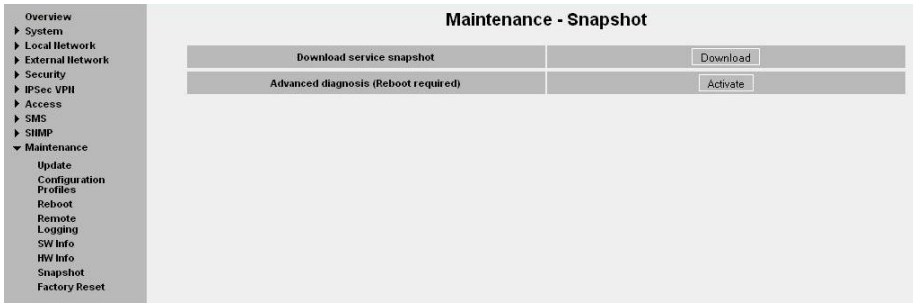
Factory setting

The factory settings for the TAINY xMOD are as follows:

Enable remote logging (FTP upload)	**No (switched off)**
Time	**00:00**
FTP Server	**NONE**
Username	**guest**
Password	**guest**

9.3 Snapshot

Maintenance > Snapshot



Function

This function is used for support purposes.

The service snapshot downloads important log files and current device settings that could be important for fault diagnosis and saves them in a file.

If you contact our customer service in the event of a problem with the TAINY xMOD, in many cases they will ask you for the snapshot file.

Note

This file contains the access parameters UMTS/GPRS and the addresses of the remote station. It does not contain the username and password for access to the TAINY xMOD.

Download service snapshot

Click on download. You can select the location on the Admin PC where the snapshot file will be saved.

The filename of the snapshot file has the following structure:

<hostname>_Snapshot_<Date&TimeCode>.tgz,

e.g.: tainyHMOD_Snapshot_200711252237.tgz

Advanced diagnosis

Please only *Activate* the *Advanced diagnosis* if asked to do so by our customer service. In operation with advanced diagnosis, information is written to the diagnosis logs much more often. Some additional information is also saved. This is useful for systematic troubleshooting.

Note

When advanced diagnosis is active, the frequent write access to the non-volatile memory of the TAINY xMOD can lead to a reduction of its service life.

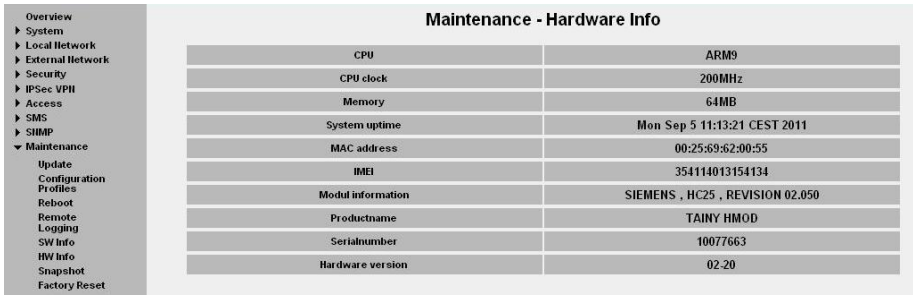
Factory setting

The factory settings for the TAINY xMOD are as follows:

Advanced diagnosis	**Off (Activate)**

9.4 Hardware information

Maintenance > Hardware Info

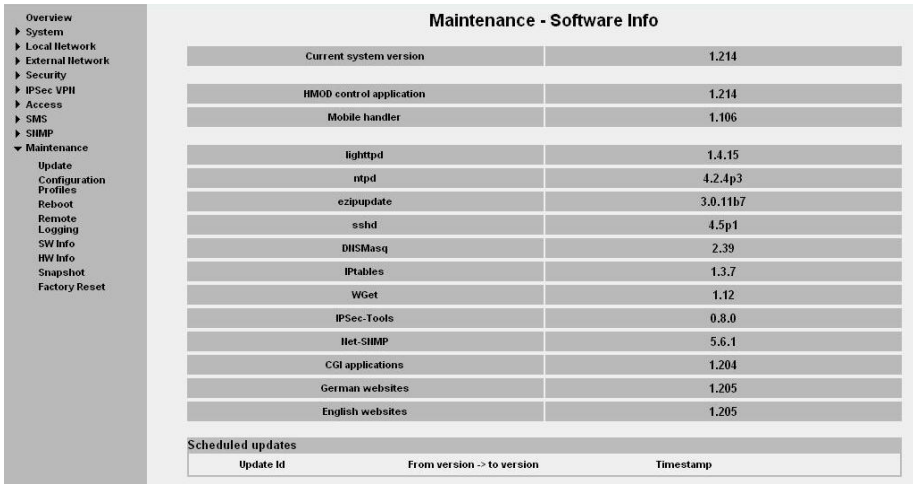


Function

Shows important information for hardware identification. This information is often needed in the event of queries to our customer service.

9.5 Software information

Maintenance > Software Info



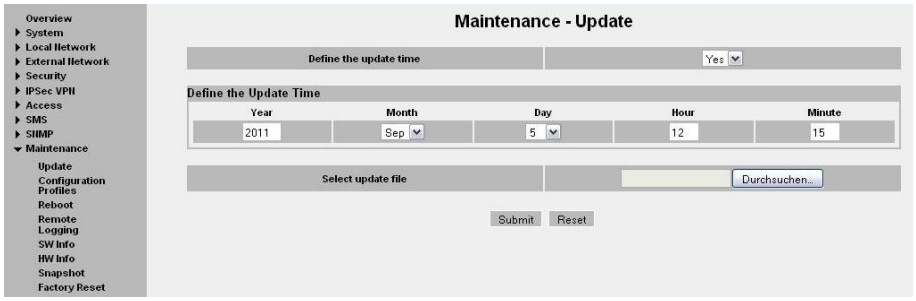
Function

Shows important information for software identification. This information is often needed in the event of queries to our customer service.

Planned updates are also shown. See also Chapter 9.6

9.6 Software Update

Maintenance > Update



Function

You can use the update function to load new operating software to the TAINY xMOD and activate this software.

The new software is unpacked during an immediate update. This process can take a few minutes. Then the actual update process begins, which is indicated by a light up of the LEDs.

The settings of the TAINY xMOD are adopted, if they still work in the new software version as they did before the update.

Define the update time

No Immediate update - The new operating software is activated immediately after you load it and click on the *Send* button.

Yes Scheduled update - The new operating software is operated at a specified update time. For this purpose, the software must be loaded in advance.

If you wish to specify the time for the update, enter the time at which the new software should be activated.

Enter the year – month – day – hour – minute.

The settings of the TAINY xMOD are adopted, if they still work in the new software version as they did before the update.

Select update file

Select the new operating software with *Browse*. For example, operating software for the TAINY xMOD has the following name:

HMOD_V2IO_v1.107-v1.214.tgz

Load the firmware to the device with *Open*.

Send

Send activates the operating software, either immediately or at the specified time.

10 Additional functions

10.1 SMS Service Center

SMS Service Center

The TAINY xMOD uses the Short Message Service (SMS) of GSM. It is possible to define a certain SMS Center.

SMS service center call number

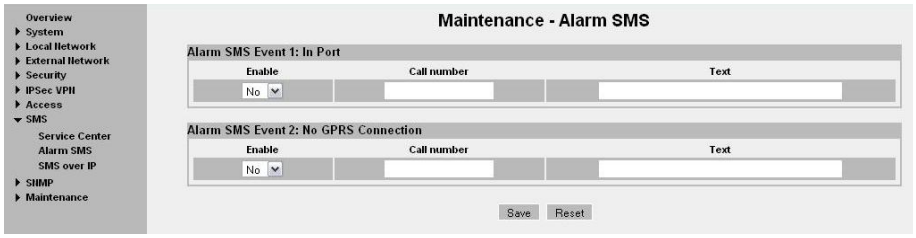
So that the SMS function will function reliably, enter the call number of the service center here. Without an entry in this location the default SMS service center of your network operator will be used.

Attention:

If no call number is entered for the SMS center or the entry is not made in the international format (e.g. +49...), then the SMS cannot be sent.

10.2 Alarm SMS

SMS > Alarm SMS



Function

The TAINY xMOD can transmit short alarm messages via the SMS (= Short Message Service) of the GSM network. Two events can trigger transmission of an alarm message via SMS:

- Event 1: In port is activated
- Event 2: No UMTS/GPRS connection

A separate call number for sending the alarm message to can be specified for each of these two events. The text of the alarm message can also be freely defined. The following characters are available: A-Z a-z 0123456789,!?

Alarm SMS Event 1: In Port

Event 1: the In port switches from inactive to active, i.e. sufficient switching voltage is applied at the In port. This function can be used, for example to transmit alarm messages of the local applications outside of the IP data connections.

Alarm SMS Event 2: No GPRS Connection

Event 2: the UMTS/GPRS connection is not established despite multiple attempts. The TAINY xMOD then transmits an alarm message.

Settings

Enable With *Yes* the alarm message is sent when the event occurs, with *No* it is not.

Call number Here enter the call number of the end device to which the alarm message is to be sent via SMS. The end device must support SMS reception via GSM or fixed network.

Text Here enter the text that should be sent as an alarm message.

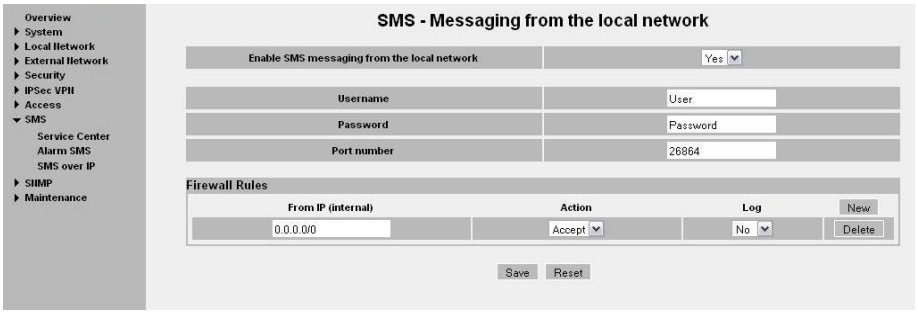
Factory setting

The factory settings for the TAINY xMOD are as follows:

SMS service center call number	**-**
Alarm SMS Event 1: In Port	**No (switched off)**
Call number	**-**
Text	**-**
Alarm SMS Event 2: No GPRS connection	**No (switched off)**
Call number	**-**
Text	**-**

10.3 SMS – Messaging from the local network

SMS > Messaging from the local network



Function

Applications being connected to the local interface of the TAINY xMOD can send messages to the TAINY xMOD which are forward then as Short Messages (SMS) via GSM.

To transmit a SMS the application at the local interface has to set-up a TCP/IP connection to the TAINY HMOD-V2-IO.

The application sends via the TCP/IP connection the text of the SMS to the TAINY xMOD. TAINY xMOD put the text in a SMS and transmits it via GSM.

Framing over the TCP/IP connection

The text has to be send to the TAINY xMOD via the TCP/IP connection using the following frame format:

Username#Password#CommandCode#Seq-Num;Phonenumber;Text:

Example: user#password#105#01;0049043465789;MySMS Text:

Username

Username to check the right to send SMS. 10 characters maximum.

Password

Password to check the right to send SMS. 10 characters maximum.

CommandCode

Command to transmit SMS from the local network. This value is fixed to 105 and may not be changed.

Seq-Num

The sequence number is used to distinguish several SMS tx jobs in parallel. The function is not supported yet.

The sequence number consists of 2 numeric characters between 01 and 99

Phonenumber

GSM telephone number of the SMS recipient. The GSM telephone number may not exceed 40 characters. International numbers (+49..) can be entered.

Text

SMS Text. The text may not exceed 160 characters. The following characters are available: A-Z a-z 0123456789,!?

The following characters are reserved and may not appear in the SMS text (forbidden characters):

#	Separator of the first command level
;	Separator of the second command level
:	End of message indicator

Enable SMS messaging from the local network	Click *Yes* to be able to send SMS from the local network.
Username	Username, which has to be part of the message frame, which text shall be transmitted by SMS. 10 characters maximum.
Password	Password, which has to be part of the message frame, which text shall be transmitted by SMS. 10 characters maximum.
Port number	Number of the TCP/IP port at which the TAINY xMOD accepts the TCP/IP connection for SMS messaging.
Firewall Rules	A firewall rule has to be established to allow the TCP/IP connection for SMS messaging to the TAINY xMOD. Click New to enter several sources (From IP) for TCP/IP connections for SMS messaging. Click Delete to remove connections.

From IP

Enter the IP address of the local application that is allowed to send IP packets to the external network. Do this by specifying the IP address or an IP range for the local application. 0.0.0.0/0 means all addresses.

To specify a range, use the CIDR notation - see the Glossary.

Action

Select accept to allow the TCP/IP connection for SMS messaging.

Log

For each individual firewall rule you can define whether the event should be

logged when the rule takes effect - set Log to *Yes*

or not - set Log to *No* (factory setting)

The log is kept in the firewall log, see Chapter 6.4.

Factory setting

The factory settings for the TAINY xMOD are as follows:

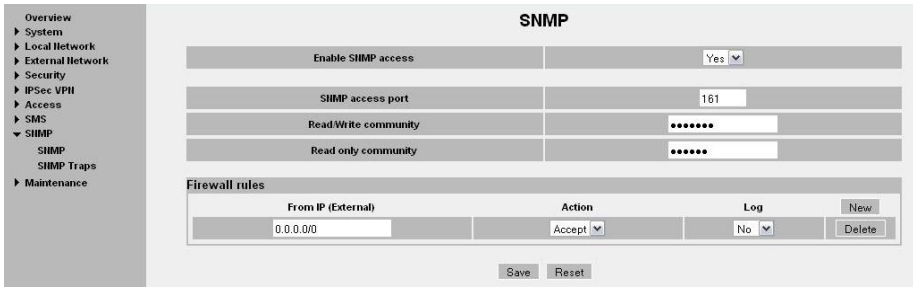
User name	**User**
Password	**Password**

Port number	**26864**
Firewall Rules	**Not active**
From IP	**0.0.0.0/0**
Action	**Accept**
Log	**No**

11 SNMP

11.1 Operation via SNMP

SNMP – SNMP



Various parameters of the TAINY xMOD can be queried or changed using SNMP Version 1 and Version 2 (Simple Network Management Protocol).

Access via SNMP can take place from both the local network and the external network.

The following SNMP queries and responses are supported by TAINY xMOD:

GET, GETNEXT, GETBULK, GETSUBTREE, WALK, SET, RESPONSE, TRAP.

The following parameters of the TAINY xMOD can be read via SNMP:

- Device identification lines (1-4)
- IP address of the external network
- PIN
- MAC address of the local interface
- Identification of the current wireless network operator
- APN
- IMSI
- IMEI
- Signal quality (CSQ value)
- Cell ID
- Cell ID of the nearby cells
- Hostname
- Maximum data volume
- Data volume of the 80% warning threshold
- Data volume currently being used (monthly volume)
- Hardware ID
- Software version
- Version number of the integrated radio module

The following parameters of the TAINY xMOD can be changed via SNMP:

- Maximum data volume (volume limit)
- PIN of the SIM card
- Device identification lines (1-4)

The exact description of the parameters is provided as a MIB (Management Information Base) on the Dr. Neuhaus website www.neuhaus.de. From there, go to the product page of the TAINY xMOD.

Enable SNMP access

Select *No* if you want to block SNMP access to the TAINY xMOD.

Select *Yes* if you want to permit SNMP access to the TAINY xMOD.

SNMP access port

Select the IP port through which the SNMP access should take place. The factory setting is the standard (Port 161).

Read / write community

Enter the SNMP community with reading and writing access rights to the TAINY xMOD.

Read-only community

Enter the SNMP community with read-only access rights to the TAINY xMOD.

Firewall rules

In order to be able to exchange data via SNMP, a firewall rule must be set upon the TAINY xMOD. New sets up multiple sources (of IP) for the UDP/IP connection. Delete removes the connections again.

From IP

Enter the IP address of the external remote location that may send IP packages to the local network. To do this, specify the IP address or an IP range of the remote location. 0.0.0.0/0 means all addresses.

Use the CIDR method to specify a range - see the glossary.

Actions

Select actions in order to enable the UDP/IP connection for SNMP.

Log

You can define each individual firewall rule for whether

the result should be logged - set Log to Yes

or not - set Log to No (factory default setting)

The protocol is written in the firewall log, see chapter 6.4.

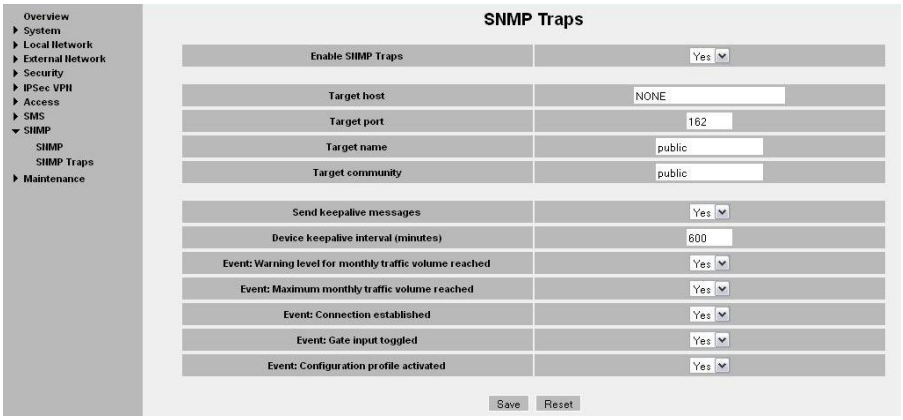
Factory settings

The TAINY xMOD has the following default settings:

Activate SNMP access	No
Port for SNMP access	161
Read / write community	public
Read-only community	public
Firewall rules	Not active
From IP	0.0.0.0/0
Actions	Allow
Log	No

11.2 Alarm messages via SNMP traps

SNMP – SNMP traps



The TAINY xMOD sends messages in the form of SNMP traps for various events.

Enable SNMP traps	Select *Yes* if you want to activate the sending of SNMP traps.
	Select *No* if you want to switch off the sending of SNMP traps.
Target host	Enter the IP address of the SNMP trap recipient.
Target port	Enter the IP port of the SNMP trap recipient.
Target name	Enter the name of the SNMP trap recipient.
Target community	Enter the name of the SNMP community here.
Send keepalive messages	Select *Yes* if you want the TAINY xMOD keepalive packages to be sent as an SNMP trap.
	Select *No* if you do not want the TAINY xMOD keepalive packages to not be sent as an SNMP trap.
Device keepalive interval (minutes)	Choose the interval which you want the keepalive SNMP traps to be sent at.
Event: Warning level for monthly traffic volume reached	Select *Yes* if you want the TAINY xMOD to send an SNMP trap upon reaching the warning threshold (80%) for the monthly data volume (see chapter 5.7).
	Select *No* if you do not want an SNMP trap to be sent for this event.
Event: Maximum monthly traffic volume reached	Select *Yes* if you want the TAINY xMOD to send an SNMP trap upon reaching the maximum monthly data volume (see chapter 5.7).
	Select *No* if you do not want to set an SNMP trap for this event.
Event: Connection re-established	Select *Yes* if you want the TAINY xMOD to send an SNMP trap when successfully re-establishing the connection to the APN.
	Select *No* if you do not want to set an SNMP trapfor this event.
Event: Gate inout toggled	Select *Yes* if you want the TAINY xMOD to send an SNMP trap with a change at the switching input.
	Select *No* if you do not want an SNMP trap to be sent for this event.
Event: Configuration profile activated	Select *Yes* if you want the TAINY xMOD to send an SNMP trap with the activation of a configuration profile.
	Select *No* if you do not want an SNMP trap to be sent for this event.

Factory settings The TAINY xMOD has the following default settings:

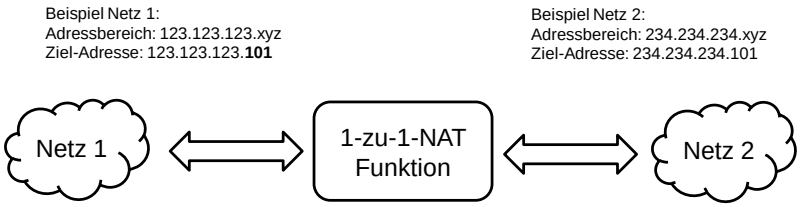
Activate SNMP traps	No

Target host	NONE
Target port	162
Target name	Public
Target community	Public
Event: Device keepalive	Yes
Device keepalive interval (minutes)	600
Event: Warning threshold for monthly volume reached	Yes
Event: Maximum monthly volume reached	Yes
Event: Re-establish connection	Yes
Event: Change at the switching input	Yes
Event: Activation of a configuration profile	Yes

12 Small lexicon of routers

1-to-1 NAT

With 1-to-1 NAT, a network component (e.g. router) maps the address range of one network to the address range of another network.



A component in Network 1 addresses a component in Network 2 through a target address from the address range of Network 1. The 1-to-1 NAT function maps the target address in the address range of Network 2. In turn, responses from Network 2 are received by a sender address from Network 1.

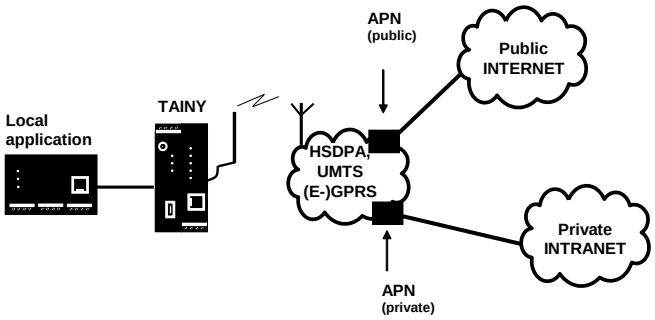
AES

Advanced Encryption Standard.

The NIST (National Institute of Standards and Technology) has developed the AES encryption standard in collaboration with industrial corporations for years. This → symmetric encryption should replace the previous DES standard. The AES standard specified three different key sizes with 128, 192 and 256 bit. In 1997 the NIST started to initiative for AES and revealed its conditions for the algorithm. From the proposed encryption algorithms the NIST narrowed the selection down to five algorithms: MARS, RC6, Rijndael, Serpent and Twofish. In October 2000 Rijndael was chosen as the encryption algorithm.

APN (Access Point Name)

Trans-network connections, e.g. from a GPRS network to the Internet, are created in the GPRS network via so-called APNs.



An end device that wants to establish a connection via the GPRS network specifies an APN to indicate which network it wants to be connected to: the Internet or a private company network that is connected via a dedicated line.

The APN designates the transfer point to the other network. It is communicated to the user by the network operator.

Asymmetric encryption

With asymmetric encryption, data is encrypted with a key and encrypted again with a second key. Both keys are suitable for encryption and decryption. One of the keys is kept secret by its owner (private key) and the other is given to the public (public key) - in other words, potential communication partners.

A message encrypted with the public key can only be decrypted and read by a recipient who has the corresponding private key. A message encrypted with the private key can only be decrypted and read by any recipient who has the corresponding public key. Encryption with the private key shows that the message actually originated from the owner of the corresponding public key. For that reason, the term “digital signature” is used.

However, asymmetric encryption processes such as RSA are slow and susceptible to certain types of attacks, which is why they are often combined with a symmetric process (→ symmetric encryption). On the other hand, concepts which eliminate the elaborate administrative efforts for symmetric keys are also possible.

CIDR

Classless Inter-Domain Routing

IP netmasks and CIDR are notations for grouping a number of IP addresses into an address space. Thus a range of contiguous addresses is treated as a network.

The CIDR method reduces, for example the routing tables stored in routers by means of a postfix in the IP address. This postfix can be used to designate a network together with its subnetworks. This method is described in RFC 1518.

In order to specify a range of IP addresses to the TAINY xMOD, or when configuring the firewall, it may be necessary to specify the address space in the CIDR notation. The following table shows the IP netmask on the left-hand side, and to the far right the corresponding CIDR notation.

IP netmask	binary	CIDR
255.255.255.255	11111111 11111111 11111111 11111111	32
255.255.255.254	11111111 11111111 11111111 11111110	31
255.255.255.252	11111111 11111111 11111111 11111100	30
255.255.255.248	11111111 11111111 11111111 11111000	29
255.255.255.240	11111111 11111111 11111111 11110000	28
255.255.255.224	11111111 11111111 11111111 11100000	27
255.255.255.192	11111111 11111111 11111111 11000000	26
255.255.255.128	11111111 11111111 11111111 10000000	25
255.255.255.0	11111111 11111111 11111111 00000000	24
255.255.254.0	11111111 11111111 11111110 00000000	23
255.255.252.0	11111111 11111111 11111100 00000000	22
255.255.248.0	11111111 11111111 11111000 00000000	21
255.255.240.0	11111111 11111111 11110000 00000000	20
255.255.224.0	11111111 11111111 11100000 00000000	19
255.255.192.0	11111111 11111111 11000000 00000000	18
255.255.128.0	11111111 11111111 10000000 00000000	17
255.255.0.0	11111111 11111111 00000000 00000000	16
255.254.0.0	11111111 11111110 00000000 00000000	15
255.252.0.0	11111111 11111100 00000000 00000000	14
255.248.0.0	11111111 11111000 00000000 00000000	13
255.240.0.0	11111111 11110000 00000000 00000000	12
255.224.0.0	11111111 11100000 00000000 00000000	11
255.192.0.0	11111111 11000000 00000000 00000000	10
255.128.0.0	11111111 10000000 00000000 00000000	9
255.0.0.0	11111111 00000000 00000000 00000000	8
254.0.0.0	11111110 00000000 00000000 00000000	7
252.0.0.0	11111100 00000000 00000000 00000000	6
248.0.0.0	11111000 00000000 00000000 00000000	5
240.0.0.0	11110000 00000000 00000000 00000000	4
224.0.0.0	11100000 00000000 00000000 00000000	3
192.0.0.0	11000000 00000000 00000000 00000000	2
128.0.0.0	10000000 00000000 00000000 00000000	1
0.0.0.0	00000000 00000000 00000000 00000000	0

Example: 192.168.1.0 / 255.255.255.0 corresponds to CIDR: 192.168.1.0/24

Client / Server

In a client/server environment, a server is a program or computer that receives queries from a client program or client computer and answers them.

In data communication, a computer that establishes a connection to a server (or host) is also referred to as a client. That means that the client is the computer that is calling and the server (or host) is the one being called.

CSD 9600

CSD (9600) stands for Circuit Switched Data or dial-in data connection. Here a connection is created between two users (end points of the connection), similar to a telephone call over a public telephone network. User 1 dials the telephone number of user 2. The network signals to user 2 that there is a call, user 2 accepts the call and the network establishes the connection until one of the users terminates the connection again.

In a GSM network this service is called CSD, and allows data transmission at 9600 bit/s or 14400 bit/s, with transmission being either secured or unsecured. Possible connections are GSM modem to GSM modem, analog modem to GSM and ISDN modem to GSM modem.

CSQ / RSSI

The CSQ value is a value defined in the GSM standard for indicating the signal quality. CSQ values correspond to the received field strength RSSI (= Received Signal Strength Indication):

CSQ	***RSSI***
< 6	< -101 dBm
6 - 10	-101 … - 93 dBm
11 – 18	- 91 dBm … -77 dBm
> 18	> 75 dBm
99	Not logged in

Datagram

In the transmission protocol TCP/IP, data are sent in the form of data packets, the so-called IP datagrams. An IP datagram has the following structure:

1. IP Header
2. TCP/UDP Header
3. Data (Payload)

The IP Header contains:

- the IP address of the sender (source IP address)
- the IP address of the recipient (destination IP address)
- the protocol number of the protocol of the next higher protocol layer (according to the OSI layer model)
- the IP Header Checksum for checking the integrity of the header upon receipt.

TCP/UDP Header contains the following information:

- the port of the sender (source port)
- the port of the recipient (destination port)
- a checksum for the TCP Header and a few items of information from the IP Header (source and destination IP addresses, etc.

DES / 3DES

The symmetric encryption algorithm (→ symmetric encryption) DES, originating from IBM and tested by the NSA, was established in 1997 by the American National Bureau of Standards, the predecessor to today's National Institute of Standards and Technology (NIST) as a standard for American governmental institutions. Since it was the first standardised encryption algorithm, it was also quickly adopted in industrial applications in the US and beyond.

DES works with a key length of 56bit, which can no longer be considered to be secure due to the increase in computing capability of the computer since 1977.

3DES is a variant of DES. It works with keys three times the size, which are 168 bits long. It is still considered to be secure and is also a part of the IPsec standard, among other things.

DHCP

The Dynamic Host Configuration Protocol (DHCP) performs automatic dynamic assignment of IP addresses and other parameters in a network. The Dynamic Host Configuration Protocol uses UDP. It was defined in RFC 2131 and was assigned the UDP ports 67 and 68. DHCP uses the client – server method, in which the client is assigned the IP addresses by the server.

DNS

Addressing in IP networks is always by means of IP addresses. It is generally preferable, however, to specify the addressing in the form of a domain address (i.e. in the form www.abc.xyz.de). If the addressing is by means of the domain address, then the sender first sends the domain address to a domain name server (DNS) and gets back the associated IP address. Only then does the sender address its data to this IP address.

DynDNS provider

Also *Dynamic DNS provider*. Every computer that is connected to the Internet has an IP address (IP = Internet Protocol). An IP address consists of up to 4 three-digit numbers, with dots separating each of the numbers. If the computer is online via the telephone line via modem, ISDN or ADSL, then the Internet service provider dynamically assigns it an IP address, i.e. the address changes from session to session. Even if the computer is online for more than 24 hours without interruption (e.g. in the case of a flat rate), the IP address is changed periodically.

For a local computer to be accessible via the Internet, its address must be known to the external remote station. This is necessary for it to establish a connection to the local computer. This is not possible, however, if the address of the local computer constantly changes. It is possible, however, if the user of the local computer has an account with a DynamicDNS provider (DNS = Domain Name Server).

Then he can specify there a hostname under which the computer can be accessed in the future, e.g.: www.xyz.abc.de. Moreover, the DynamicDNS provider makes available a small program that has to be installed and executed on the computer concerned. In each Internet session of the local computer this tool reports to the DynamicDNS provider which IP address the computer has at the moment. Its domain name server registers the current hostname - IP address assignment and reports this to other domain name servers in the Internet.

If now an external computer wants to establish a connection with a local computer which is registered with the DynamicDNS provider, the external computer uses the hostname of the local computer as the address. In this way a connection is established with the responsible DNS (Domain Name Server) in order to look up there the IP address which is currently assigned to this hostname. The IP address is transmitted back to the external computer, and then used by it as the destination address. This now leads precisely to the desired local computer.

As a rule, all Internet addresses are based on this method: First a connection is established to a DNS in order to determine the IP addresses assigned to this hostname. Once that has been done, the IP address that was "looked up" is used to establish the connection to the desired remote station, which can be any Web site.

EDGE

EDGE (= Enhanced Data Rates for GSM Evolution) refers to a method in which the available data rates in GSM mobile phone networks are increased by introducing an additional modulation process. With EDGE, GPRS is expanded to become EGPRS (Enhanced GPRS), and HSCSD is expanded to become ECSD.

EGPRS

EGPRS stands for "Enhanced General Packet Radio Service", which describes a packet-oriented data service based on GPRS, which is accelerated by means of EDGE technology.

GPRS

GPRS is the abbreviation for "General Packet Radio Service", a data transmission system of GSM2+ mobile phone systems. GPRS systems use the base stations of GSM networks as their wireless equipment, and their own infrastructure for coupling to other IP networks, such as the Internet. Data communication is packet-oriented; the Internet Protocol (IP) is used. GPRS provides data rates of up to 115.2 Kbit/s.

GSM

GSM (= Global System for Mobile Communication) is a standard that is used worldwide for digital mobile phone networks. In addition to the voice service for telephone calls, GSM supports various data services, such as fax, SMS, CSD and GPRS. Depending on the legal requirements in the various countries, the frequency bands 900 MHz, 1800 MHz or 850 MHz and 1900 MHz are used.

HSDPA

HSDPA (=High Speed Downlink Packet Access) is an extension of the UMTS network, which provides higher data rates from the base station to the mobile station.

HTTPS

HTTPS (=HyperText Transfer Protocol Secure) is a variant of the familiar HTTP, which is used by any Web browser for navigation and data exchange in the Internet. For example, this familiar entry : http://www.neuhaus.de.

In HTTPS the original protocol is supplemented with an additional component for data protection. While in HTTP data are transmitted unprotected in plain text, in HTTPS data are transmitted only after an exchange of digital certificates, and in encrypted form.

IP address

Every host or router on the Internet / an intranet has a unique IP address (IP = Internet Protocol). The IP address is 32 bits (= 4 bytes) long, and is written as 4 numbers (each in the range from 0 to 255), which are separated from each other by dots.

An IP address has 2 parts: the network address and the host address.

All hosts of a network have the same network address, but different host addresses. Depending on the size of the network in question - a distinction is made between networks of Class A, B and C - the two address components may be of different sizes:

	1st byte	2nd byte	3rd byte	4th byte
Class A	Netw. addr.	Host addr.		
Class B	Netw. addr.		Host addr.	
Class C	Netw. addr.			Host addr.

It can be seen from the first byte of the IP address whether the IP address designates a network of Class A, B or C. The following definitions apply:

	Value of the 1st byte	Bytes for the network address	Bytes for the host address
Class A	1-126	1	3
Class B	128-191	2	2
Class C	192-223	3	1

If you do the arithmetic, you can see that there can be a maximum of 126 Class A networks worldwide, and each of these networks can comprise a maximum of 256 x 256 x 256 hosts (3 bytes of address space). There can be 64 x 256 Class B networks, each of which can contain up to 65,536 hosts (2 bytes of address space: 256 x 256). There can be 32 x 256 x 256 Class C networks, each of which can contain up to 256 hosts (1 byte of address space).

IP packet

See Datagram

IPsec

IP security (IPsec) is a standard which uses IP datagrams to ensure the authenticity of the sender, the confidentiality and the integrity of the data through encryption. The components of IPSec are the authentication Header (AH), the encapsulating security payload (ESP), the security association (SA), the security parameter index (SPI) and the internet key exchange (IKE).

At the beginning of the communication, the computers participating in the communication clarify the process used and its implications, such as transport mode or tunnel mode.

In transport mode, an IPSec header is used between the IP header and TCP or UDP header in each IP datagram. Since the IP header remains unchanged in the process, this mode is only suitable for a host-to-host connection.

In tunnel mode, an IPSec header and a new IP header precede the entire IP datagram. That means the original datagram is encrypted in the payload of the new datagram.

Tunnel mode is used with the APN: The devices at the tunnel ends encrypt and decrypt the datagrams along the stretch of the tunnel; in other words, the actual datagrams are fully protected along the transport route through the public network.

MIB

See SNMP

NAT (Network Address Translation)

With network address translation (NAT), often called IP masquerading, an entire network is "hidden" behind a single device, known as the NAT router. The internal computers in the local network remain concealed with their IP addresses in the local network when they communicate outwardly through the NAT router. Only the ANT router with its own IP address is visible to outside communication partners.

However, in order for internal computers to be able to communicate directly with external computers (on the internet), the NAT router must change the IP datagrams to and from the internal computer to the outside.

If an IP datagram is sent from the internal network to the outside, the NAT router changes the IP and TCP header of the datagram. It switches the source IP address and the source port with its own official IP address and its own, previously unused port. For this purpose, it maintains a table which establishes the allocation of the original with the new values.

Upon receiving a response datagram, the NAT router recognises that the datagram is actually intended for an internal computer on the basis of the specified target port. Using the table, the NAT router exchanges the target IP address and the target port and forwards the datagram to the internal network.

Network mask / Subnet mask

A company network with access to the Internet is normally officially assigned only a single IP address, e.g. 134.76.0.0. In this example address it can be seen from the 1st byte that this company network is a Class B network, i.e. the last 2 bytes can be used freely for host addressing. Arithmetically that represents an address space of 65,536 possible hosts (256 x 256).

Such a huge network is not very practical. It is necessary here to form subnetworks. This is done using a subnet mask. Like an IP address, this is a field 4 bytes long. The value 255 is assigned to each of the bytes that represent the network address. The main purpose of this is to "hide" a part of the host address range in order to use it for the addressing of subnetworks. For example, in a Class B network (2 bytes for the network address, 2 bytes for the host address), by means of the subnet mask 255.255.255.0 it is possible to take the 3rd byte, which was actually intended for host addressing, and use it now for subnet addressing. Arithmetically that means that 256 subnets with 256 hosts each could be created.

Port number

The Port Number field is a 2-byte field in UDP and TCP headers. The assignment of port numbers serves to identify various data flows that are processed simultaneously by UDP/TCP. The entire data exchange between UDP/TCP and the application processes takes place via these port numbers. The assignment of port numbers to application processes is performed dynamically and randomly. Fixed port numbers are assigned for certain frequently-used application processes. These are called Assigned Numbers.

PPPoE

Acronym for Point-to-Point Protocol over Ethernet. It is based on the standards PPP and Ethernet. PPPoE is a specification for connecting users to the Internet via Ethernet using a jointly used broadband medium such as DSL, Wireless LAN or cable modem.

PPTP

Acronym for Point-to-Point Tunneling Protocol. This protocol was developed by Microsoft, U.S. Robotics and others in order to transmit data securely between two VPN nodes (→ VPN) over a public network.

Private key, public key; certification (X.509)

Two keys are used with asymmetric encryption algorithms: one private (*private key*) and one public (*public key*). The public key is used for the encryption of data and the private key is used for the decryption.

The public key is provided by the future recipient of data to those who encrypt and send data to the recipient. Only the recipient has the private key. It is used for the decryption of the data received.

Certification:

The possibility of certification exists so that the user of the public key (used for encryption) can be certain that the public key really originated from the party who was intended to receive the data to be sent: a certification authority (*CA*) checks the authenticity of the public key and the associated linking of the sender's identity with its key. This is conducted according to the CA's rules, which may require the sender to appear in person. After a successful check, the CA signs the public key of the sender with its (digital) signature. A *certificate* is created.

An X.509 certificate establishes a link between an identity in the form of an "X.500 distinguished name" (DN) and an official key, which is certified with the digital signature of an X.509 certification authority (CA). The signature (an encryption with the signature key) can be checked with the public key which the CA issues to the certificate holder.

Protocol, Transfer protocol

Devices that communicate with each other must use the same rules. They have to "speak the same language". Such rules and standards are called protocols or transfer protocols. Frequently used protocols include IP, TCP, PPP, HTTP and SMTP. TCP/IP is the umbrella term for all protocols that are based on IP.

Service provider

Supplier, company or institution that gives users access to the Internet or to an online service.

Spoofing, Anti-Spoofing

In Internet terminology, spoofing means to specify a forged address. The forged Internet address is used to pose as an authorised user.

Anti-spoofing means mechanisms to reveal or prevent spoofing.

SNMP

SNMP (Simple Network Management Protocol) is a widespread mechanism for the central control of network components such as servers, routers, switches, printers, computers etc.

SNMP defines the communication process and the structure of the data packages. UDP via IP is used for the transport.

SNMP does not define the values which can be read or changed.

This is done in an MIB (Management Information Base). The MIB is a description file in which the individual values are listed in a table. The MIB is for specific network components or for a class of components, such as switches.

SNMP Trap

SNMP trap is a message which is sent unprompted by the SNMP agent (Simple Network Management Protocol) from a network component.

SSH

SSH (Secure SHell) is a protocol that enables secure, encrypted data exchange between computers. Secure SHell is used for remote access to the input console from LINUX-based machines.

Symmetric encryption

With symmetric encryption, data is encrypted and decrypted with the same key. DES and AES are two examples of symmetric encryption algorithms. They are fast, but time-consuming to administer as the number of users increases.

TCP/IP (Transmission Control Protocol/Internet Protocol

Network protocol that is used to connect two computers on the Internet.

IP is the basic protocol.

UDP builds on IP, and sends individual packets. These can arrive at the recipient in a different sequence from the one they were sent in, or they can even get lost.

TCP serves to secure the connection, and ensures, for example, that the data packets are forwarded to the application in the right sequence.

UDP and TCP provide, in addition to the IP addresses, port numbers between 1 and 65535, which can be used to distinguish the various services.

A number of additional protocols are based on UDP and TCP, such as HTTP (Hyper Text Transfer Protocol), HTTPS (Secure Hyper Text Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol, Version 3), DNS (Domain Name Service).

ICMP builds on IP, and contains control messages.

SMTP is an e-mail protocol based on TCP.

IKE is an IPsec protocol based on UDP.

ESP is IPsec protocol based on IP.

On a Windows PC, WINSOCK.DLL (or WSOCK32.DLL) handles both of these protocols.

(→ Datagram)

UDP

See TCP/IP

UMTS

UMTS (Universal Mobile Telecommunication System) is a 3rd generation mobile radio network, which allows significant higher data transmission rates, than the 2nd generation GSM networks. UMTS provides beside voice connections also IP-based data connections, SMS transmission and high speed data application like video.

Accept in North American area UMTS uses a frequency band at 2100 MHz. In North America the frequency bands at 850 MHz and 1900 MHz are used, which are also used for GSM networks.

VPN (Virtual Private Network)

A virtual private network (VPN) connects several physically separate private networks (subnetworks) through a public network, such as the internet to form a common network. The use of cryptographic protocols ensures confidentiality and authenticity. A VPN thus offers an affordable alternative to standard lines for creating a supraregional company network.

X.509 certificate

A type of "seal" which verifies the authenticity of the public key (→ asymmetric encryption) and corresponding data.

The possibility of certification exists so that the user of the public key (used for encryption) can be certain that the public key really originated from its actual originator and thus from the party who was intended to receive the data to be sent. A certification authority (CA) checks the authenticity of the public key and the associated linking of the originator's identity with its key. This takes place according to the CA's rules, which may require the originator of the public key to appear in person. After a successful check, the CA signs the public key with its (digital) signature. A certificate is created.

An X.509(v3) certificate thus contains a public key, information about the owner of the key (specified by distinguished name [DN]), allowed purposes of use, etc. and the signature of the CA.

The signature is created as follows: The CA creates an individual bit sequence up to 160 bits long known as the HASH value from the public key's bit sequence, the data on its owner and from additional data. The CA encrypts this with its private key and adds the certificate. Encryption with the CA's private key verifies authenticity, meaning that the encrypted HASH character sequence is the CA's digital signature. If the data of the certificate appears to have been manipulated, this HASH value will no longer be correct and the certificate will be worthless.

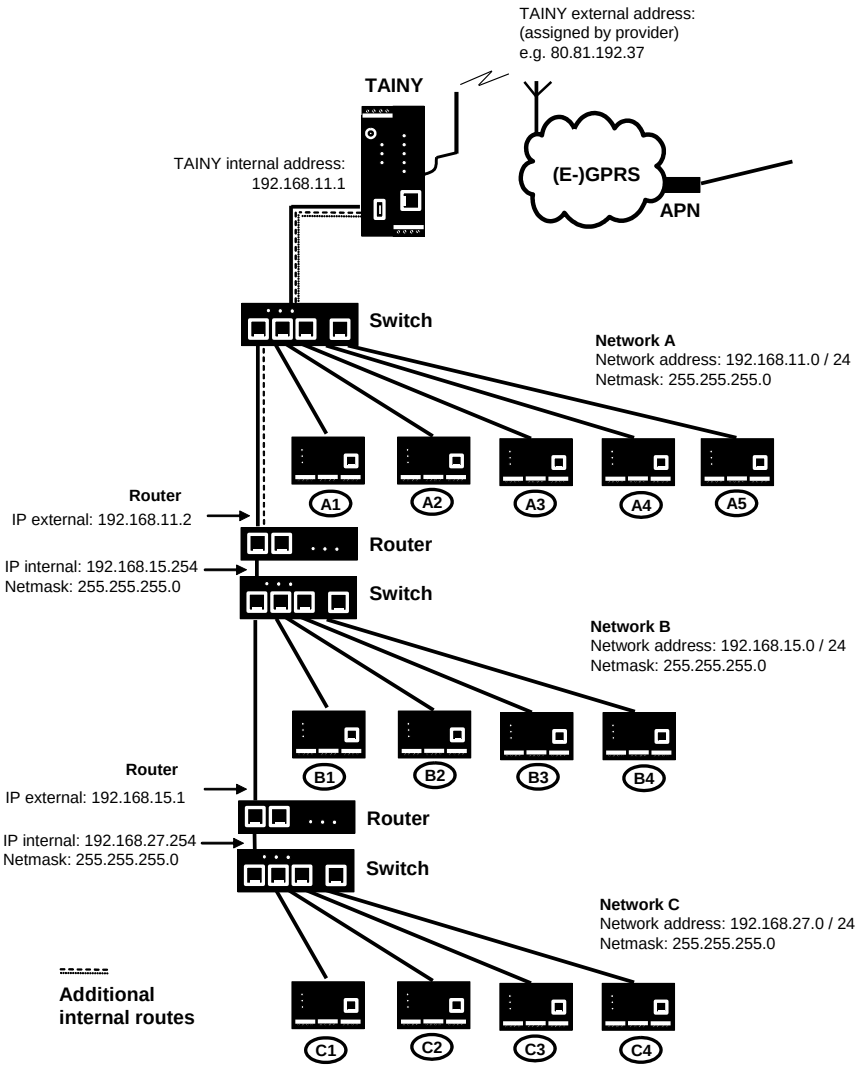
The HASH value is also referred to as a fingerprint. Since it is encrypted with the CA's private key, anyone who has the appropriate public key can encrypt the bit sequence and thus check the authenticity of this fingerprint or this signature.

By using the services of authentication authorities, it is possible that one key owner need not know the other, only the authentication authority. The additional information for the key also simplifies the administrative efforts for the key.

X.509 certificates are used for email encryption, etc. using S/MIME or IPsec.

Additional Internal Routes

The following sketch shows how the IP addresses could be distributed in a local network with subnetworks, what network addresses result from this, and what the specification for an additional internal route could look like.



Network A is connected to the TAINY HMOD-V2-IO and via it to a remote network. Additional internal routes show the path to additional networks (networks B, C), which are connected to each other via gateways (routers). For the TAINY HMOD-V2-IO, in the example shown networks B and C can both be reached via gateway 192.168.11.2 and network address 192.168.11.0/24.

Network B					
Computer	B1	B2	B3	B4	**Additional internal routes:** Network: 192.168.15.0/24 Gateway: 192.168.11.2 Network: 192.168.27.0/24 Gateway: 192.168.11.2
IP address	192.168.15.3	192.168.15.4	192.168.15.5	192.168.15.6	
Network mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	
Network C					
Computer	C1	C2	C3	C4	
IP address	192.168.27.3	192.168.27.4	192.168.27.5	192.168.27.6	
Network mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	

13 Technical data

13.1 TAINY HMOD-V2-IO, TAINY HMOD-L1-IO

Interfaces	Application interface	10/100 Base-T (RJ45 plug) Ethernet IEEE802 10/100 Mbit/s
	Service interface	USB-A (reserved for later applications)
Security functions	VPN	VPN IPSec (TAINY HMOD-V2-IO only) Such as 10 VPN tunnel
	Firewall	Stateful inspection firewall Anti-spoofing Port forwarding
Additional functions		DNS cache, DHCP server, NTP, remote logging, connection monitoring, alarm-SMS
Management		Web-based administration user interface, SSH console
Wireless connection	Frequency bands	UMTS/HSDPA: Triple band, 850//1900/2100MHz GSM/GPRS/EDGE: Quad band, 850/900/1800/1900MHz
	HSDPA	3.6 Mbps, UL 384 kbps UE CAT. [1-6], 11, 12 supported Compressed mode (CM) supported according to 3GPP TS25.212
	UMTS	PS data rate – 384 kbps DL / 384 kbps UL CS data rate – 64 kbps DL / 64 kbps UL
	EDGE (EGPRS)	EDGE Multislot class 12 / EDGE Multislot class 12 Multislot Class 10 Mobile Station Class B PBCCH support Downlink coding schemes – CS 1-4, MCS 1-9 Uplink coding schemes – CS 1-4, MCS 1-9
	GPRS	Multislot Class 10 Full PBCCH support Mobile Station Class B Coding Scheme 1 – 4
	CSD / MTC	V.110, RLP, non-transparent 9.6 kbps
	SMS (TX)	Point to point, MO (outgoing)
	Antenna connection	Nominal impedance: 50 ohms, jack: SMA
Ambient conditions	Temperature range	Operation: -20 °C to +60 °C Storage: -40 °C to +70 °C
	Air humidity	0-95 %, non-condensing

Housing	Design	Top-hat rail housing
	Material	Plastic
	Protection class	IP20
	Dimensions	114 mm x 45 mm x 99 mm
	Weight	approx. 280g
Conformity	CE	Conforms to Directive 99/05/EC
	GSM / UMTS	Applied standard: EN301 511 v.9.0.2, EN301 908-1/-2: v.4.2.1
	GSM/EGPRS module	Conforms to GCF, PTCRB
	EMC/ESD	Applied standards: EN 55022:2010 Klasse A, EN 55024: 1998 + A1:2001 + A2:2003, EN 61000-6-2:2005
	Electrical safety	Applied standard: EN 60950:2006 + A11:2009 + A1:2010
	Environment	The device complies with the European Directives RoHS and WEEE.
Power supply	Input voltage	12 - 60 V DC (24 V DC nominal)
	Power input	4.4 W typical at 12 V 4.0 W typical at 24 V 5.5 W typical at 60 V
	Supply current	450mA at 12V and 100mA at 60V Iburst = 1.26A

13.2 TAINY EMOD-V2-IO, TAINY EMOD-L1-IO

Interfaces	Application interface	10/100 Base-T (RJ45 plug) Ethernet IEEE802 10/100 Mbit/s
	Service interface	USB-A (reserved for later applications)
Security functions	VPN	IPSec (TAINY HMOD-V2-IO only)
	Firewall	Stateful inspection firewall Anti-spoofing Port forwarding
Additional functions		DNS cache, DHCP server, NTP, remote logging, connection monitoring, alarm-SMS
Management		Web-based administration user interface, SSH console
Wireless connection	EDGE (EGPRS)	EDGE Multislot class 12 / EDGE Multislot class 12
	Coding schemes GSM Module	CS-1, CS-2, CS-3, CS-4 EGPRS (EDGE) / Quad band
	EDGE (EGPRS)	Multislot Class 10 Mobile Station Class B Modulation and Coding Scheme MCS 1 – 9
	GPRS	Multislot Class 12 Full PBCCH support Mobile Station Class B Coding Scheme 1 – 4
	EDGE / GPRS	During the data transmission via EGPRS or GPRS, the device automatically chooses between the following classes: - from EGPRS Multislot Class 12 (4Tx slots) to EGPRS Multislot Class 10 (2Tx slots), - from EGPRS Multislot Class 10 (2Tx slots) to EGPRS Multislot Class 8 (1Tx), - from GPRS Multislot Class 12 (4Tx slots) to GPRS Multislot Class 8 (1Tx) from GPRS Multislot Class 10 (2Tx slots) to GPRS Multislot Class 8 (1Tx)
	CSD / MTC	V.110, RLP, non-transparent 2.4, 4.8, 9.6, 14.4kbps
	SMS (TX)	Point to point, MO (outgoing)
	Max. transmission power (in accordance with output 99, V5)	Class 4 (+33dBm ±2dB) for EGSM850 Class 4 (+33dBm ±2dB) for EGSM900 Class 1 (+33dBm ±2dB) for EGSM850 Class 1 (+30dBm ±2dB) for GSM1900 Class E2 (+27dBm ± 3dB) for GSM 850 8-PSK Class E2 (+27dBm ± 3dB) for GSM 900 8-PSK

		Class E2 (+26dBm +3 /-4dB) for GSM 1800 8-PSK Class E2 (+26dBm +3 /-4dB) for GSM 1900 8-PSK
	Antenna connection	Nominal impedance: 50 ohms, jack: SMA
Ambient conditions	Temperature range	Operation: -20 °C to +60 °C Storage: -40 °C to +70 °C
	Air humidity	0-95 %, non-condensing
Housing	Design	Top-hat rail housing
	Material	Plastic
	Protection class	IP20
	Dimensions	114 mm x 45 mm x 99 mm
	Weight	approx. 280g
Conformity	CE	Conforms to Directive 99/05/EC
	GSM / UMTS	Applied standard: EN301 511 v.9.0.2
	GSM/EGPRS module	Conforms to GCF, PTCRB
	EMC/ESD	Applied standards: EN 55022:2010 Klasse A, EN 55024: 1998 + A1:2001 + A2:2003, EN 61000-6-2:2005
	Electrical safety	Applied standard: EN 60950:2006 + A11:2009 + A1:2010
	Environment	The device complies with the European Directives RoHS and WEEE.
Power supply	Input voltage	12 - 60 V DC (24 V DC nominal)
	Power input	4.4 W typical at 12 V 4.0 W typical at 24 V 5.5 W typical at 60 V
	Supply current	450mA at 12V and 100mA at 60V Iburst = 1.26A